Chicago Journal of International Law

Volume 18 | Number 1 Article 1

7-1-2017

The Law of Cyber Peace

Scott J. Shackelford

The Law of Cyber Peace

Scott J. Shackelford, JD, PhD*

Abstract

Scholars and policymakers are paying greater attention to the application of international law to the cause of enhancing global cybersecurity. The bulk of this research, though, has been focused on leveraging international humanitarian law to regulate the conduct of cyber warfare. Yet much of this work is largely theoretical, given how exceedingly rare it is for a cyber attack to cross the armed-attack threshold at which point the law of armed conflict is activated. Most of the cyber risk facing the public and private sectors lies in the arena of cybercrime and espionage. More scholars have been applying international law 'below the threshold' to these issues, but much more work remains to be done. This Article seeks to address this omission by offering a roadmap that synthesizes and extends work in this field. The time is ripe for a fresh look at existing international legal tools that would help us better manage the multifaceted cyber threat. Only then can an accounting be made of gaps to be filled in by norms, custom, and perhaps one day, new accords.

Table of Contents

* Associate Professor, Indiana University; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Research Fellow, Harvard Kennedy School Belfer Center for Science and International Affairs; Senior Fellow, Center for Applied Cybersecurity Research.

I. INTRODUCTION

In December 2014, Sony Pictures was the victim of a data breach, allegedly by a group of hackers known as the "Guardians of Peace" with ties to the North Korean regime.[1] The breach sparked a wave of partisan commentary, with President Obama calling the incident an example of "cyber vandalism," while Senator John McCain called it "the manifestation of a new kind of warfare."[2] This episode highlights the difficulty of classifying cyber operations under international law, given the widely divergent views that can result from the same fact pattern. Cybersecurity often seems to be in the eye of the beholder. This begs the question as to what is the most appropriate legal framework for guiding policymakers' responses to such incidents. This can be a particularly vexing question for incidents below the armed attack threshold, at which point the law of armed conflict is activated, and which is also where the vast majority of cyber operations fall,[3] from the now infamous 2015 U.S. Office of Personnel Management (OPM) breach to more recent attacks on the South Korean subway, Cisco, and the SWIFT code system relied on by myriad financial firms.[4] Yet it is also an arena in which international attention is increasingly being paid. This may be seen by the governance spectrum of State approaches to enhancing cybersecurity as well as norm-building efforts such as the 2015 G20 communique on the applicability of international law to cyberspace,[5] the 2016 G7 cybersecurity statement,[6] and the G2 cybersecurity code of conduct.[7]

Increasing and worthwhile attention has been paid to applying existing international law to the cause of enhancing global cybersecurity. The bulk of this research, though, has been focused on leveraging international humanitarian law

---

1 *See, for example*, Steve Holland & Doina Chiacu, *Obama Says Sony Hack Not an Act of War*, REUTERS (Dec. 22, 2014), https://perma.cc/8N7Y-LW3A.

2 *Id.*

3 *See* Brandon Valeriano & Ryan C. Maness, *The Coming Cyberspace: The Normative Argument Against Cyberwarfare*, FOREIGN AFFAIRS (May 13, 2015), https://perma.cc/9NMQ-4B2Q ("Despite fears of a boom in cyberwarfare, there have been no major or dangerous hacks between countries.").

4 *See* Sara Sorcher, *OPM Breach a Shadow Over Homeland Security's Appeals to Security Pros*, CHRISTIAN SCI. MONITOR (Aug. 7, 2015), https://perma.cc/XS4F-5Z6H; Shannon Hayden, *Cyber Attack on South Korean Subway System Could Be a Sign of Nastier Things to Come*, VICE NEWS (Oct. 8, 2015), https://perma.cc/24QP-4V3R; Warwick Ashford, *Cisco Praised for Quick Response to Cyber Attack*, COMPUTER WEEKLY (Oct. 8, 2015), https://perma.cc/LH92-UKEU.

5 *See* G20 LEADERS' COMMUNIQUÉ, ANTALYA SUMMIT (Nov. 15–16, 2015), https://perma.cc/BU57-9XKX.

6 *G7 Leaders Approve Historic Cybersecurity Agreement*, BOS. GLOBAL F. (June 6, 2016), https://perma.cc/RM3S-FZ2W.

7 *See* Teri Robinson, *U.S., China Agree to Cybersecurity Code of Conduct*, SC MAG. (June 26, 2015), https://perma.cc/K9GQ-FZPT.

to regulate the conduct of cyber warfare.[8] Yet much of this work is largely hypothetical given how exceedingly rare it is for a cyber operation to cross the armed attack threshold.[9] The majority of the cyber risk facing the public and private sectors lies in the arena of cybercrime and espionage.[10] More scholars have been applying international law "below the threshold" to these issues as may be seen by the *Tallinn 2.0* project,[11] but much more work remains to be done.[12] For example, perhaps surprisingly, relatively little literature exists examining the potential to leverage private international law to the cause of mitigating global cyber risk.[13]

This Article seeks to help address this omission by offering a roadmap that synthesizes and extends work in this field. It does so by drawing from cybersecurity due diligence, cyber risk insurance, project finance, voluntary frameworks, trade, investment treaties, and underexplored realms of public international law including the Vienna Convention on Diplomatic Relations, global commons regimes, and Mutual Legal Assistance Treaties (MLATs).[14] The time is ripe for a fresh look at existing international legal tools that would help us better manage the multifaceted cyber threat. Only then can an accounting be made of gaps to be filled in by norms, ethics, custom, and perhaps one day, new accords. This work is meant to be a follow-up study to another article analyzing the applicable international law to cyber operations both above and below the armed

---

8 *See, for example*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICATION TO CYBER WARFARE 17 (Michael N. Schmitt ed., 2013) (discussing when a cyber attack could trigger the right of self-defense) [hereinafter TALLINN MANUAL].

9 *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 34, 67 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009) [hereinafter NATIONAL ACADEMIES]. There are varying interpretations for defining the jus in bello threshold for armed attacks under international law, but the most common is arguably the equivalent effects test, which requires that for a cyber operation to be an armed attack, it must have results equivalent to a physical invasion by traditional military forces.

10 *See, for example*, Scott J. Shackelford, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 3–51 (2014).

11 TALLINN 2.0, https://perma.cc/G6GB-PPQP (last visited Aug. 9, 2015). TALLINN 2.0 seeks to unpack the public international law applicable below the armed attack threshold, representing a follow-up from the widely-discussed TALLINN MANUAL. *See* TALLINN MANUAL, *supra* note 8; Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 698 (2014).

12 *But see* Michael N. Schmitt & Sean Watts, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, 21 J. of CONFLICT & SEC. L. 1, 1 (2016) (unpacking the role of non-state actors in international cybersecurity).

13 *Cf.* Teresa Scassa & Robert J. Currie, *New First Principles? Assessing the Internet's Challenges to Jurisdiction*, 42 GEO. J. INT'L L. 1017, 1030–31 (2011); Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1194 (2014).

14 *See generally* Scott J. Shackelford, *From Net War to Nuclear War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192 (2009).

attack threshold, taking into account legal development in the preceding seven years.[15] It is also a summation of an array of stand-alone efforts investigating various aspects of the law of cyber peace into a coherent whole while breaking new conceptual ground, particularly in the rapidly evolving field of private international cybersecurity law as one component of a "polycentric" approach to promoting cyber peace.[16]

This Article is structured as follows. Section II reviews the private international law applicable to the cause of promoting a global culture of cybersecurity, including the rise of "voluntary" cybersecurity risk frameworks.[17] Section III analyzes the applicable public international law below the armed attack threshold. Finally, Section IV investigates the role that cybersecurity norms may play as legal harmonization proceeds, along with examining proposed

---

15 *See id.*

16 *See* Scott J. Shackelford & Timothy L. Fort, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2032 (2016); Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 50 (2016); Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653, 711 (2016); Scott J. Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace: Analyzing the Current State and Impact of National Cybersecurity Strategies on Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895, 941–42 (2015); Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 259–60 (2016); Scott J. Shackelford & Zachary Bohm, *Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation*, 40 CAN.-U.S. L.J. 61, 69–70 (2016); Scott J. Shackelford, *Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAPMAN L. REV. 445, 464–65 (2016); Amanda N. Craig, Scott J. Shackelford, & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 786–87 (2015); Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 354–55 (2015); Eric Richards, Scott J. Shackelford, & Abbey Stemler, *Rhetoric Versus Reality: U.S. Resistance to Global Trade Rules and the Implications for Cybersecurity and Internet Governance*, 24 MINN. J. INT'L L. 159, 173 (2015); Scott J. Shackelford & Scott Russell, *Risky Business: Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy*, 24 MINN. J. INT'L L. 1, 14–15 (2015); Scott J. Shackelford & Scott Russell, *Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector*, 10 FIU. L. REV. 635, 667 (2015); Scott J. Shackelford, Timothy L. Fort, & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353, 430–31 (2014); Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace and Safeguarding Trade Secrets through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 73–4 (2015); Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 184 (2014); Amanda N. Craig & Scott J. Shackelford, *Hacking the Planet, the Dalai Lama, and You: Managing Technical Vulnerabilities in the Internet through Polycentric Governance*, 24 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 381, 423–25 (2014); Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1360–64 (2013); Shackelford, *supra* note 14.

17 John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG. (2014), https://perma.cc/8CLX-YBQC.

cybersecurity accords and the role that polycentric governance may play in fostering cyber peace.[18]

II. THE PRIVATE INTERNATIONAL LAW OF CYBER PEACE

International law has been defined as "the body of legal rules," norms, and standards that applies "between sovereign States" and non-State actors, including international organizations and multinational companies, enjoying legal personality.[19] Traditionally, the primary sources of international law include treaties, custom,[20] and general principles of law.[21] Subsidiary sources of international law include judicial decisions and scholarly writing.[22] Given the recent nature and rapid development of cyber-capabilities, there are comparatively few treaties that specifically address the rights and obligations of States vis-à-vis cybersecurity, with the notable exception of the Council of Europe Convention on Cybercrime (Budapest Convention) discussed below.[23] Absent a robust treaty regime, and given the geopolitical difficulties of negotiating new agreements in this area,[24] it is vital to clarify the role of existing private and public international law related to the promotion of cyber peace.

Private international law is a far-reaching and often underappreciated body of law.[25] Although myriad definitions exist, the Organization of American States has defined private international law as "the legal framework composed of conventions, protocols, model laws, legal guides, uniform documents, case law, practice and custom, as well as other documents and instruments, which regulate

---

18 Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care, Conference on Self-Governance, Polycentricity, and Development* 1 (prepared for presentation at Renmin University, Beijing, China) (May 8, 2011), https://perma.cc/ZLF8-R3MQ; Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Hamadoun I. Toure & Perm. Monitoring Panel on Info. Sec. eds., 2011), https://perma.cc/TA8D-VEZP (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace."); SHACKELFORD, *supra* note 10, at 52–110, 312–366.

19 Malcolm Shaw, *International Law, Definition of International Law*, ENCYCLOPEDIA BRITANNICA (last visited May 03, 2017), https://perma.cc/8PJ9-JHKP.

20 Customary international law is often defined as the "general and consistent practice of states followed by them from a sense of legal obligation." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (A.L.I. 1987).

21 Statute of the International Court of Justice Art. 38, June 16, 1945, 59 Stat. 1055, 33 U.N.T.S. 933.

22 *See* MALCOLM N. SHAW, INTERNATIONAL LAW 69–71 (4th ed. 1997).

23 Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.

24 *See* Joseph S. Nye, Jr., *Power and National Security in Cyberspace*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 5, 19–20 (Kristin M. Lord & Travis Sharp eds., 2011).

25 *See* PAUL B. STEPHAN & JULIE A. ROIN, INTERNATIONAL BUSINESS AND ECONOMICS: LAW AND POLICY vii (4th ed. 2010).

relationships between individuals in an international context."[26] Given how expansive this category of law is, its potential for shaping the emerging field of international cybersecurity law is immense, ranging from cybersecurity standards and national frameworks to cybersecurity risk insurance programs, trade and investment treaties, cybersecurity due diligence, and relevant case law. Many law firms, for example, see cybersecurity devolving throughout their practice areas, including the more traditional international law practice groups of project finance, international trade, and international arbitration.[27] Space constraints prohibit a comprehensive analysis of each of these facets of private international cybersecurity law within this Article. Rather, the goal here is to begin to map out what we know and identify governance gaps to help jumpstart a broader conversation about the utility of private international law in furthering the cause of cyber peace. First, though, it is important to define core concepts, beginning with the notion of "cyber peace" itself.

A. Defining Key Terms: Unpacking a "Polycentric" "Cyber Peace"

Private-sector cybersecurity best practices, along with national, bilateral, and regional bodies acting as norm entrepreneurs that are identified throughout this study are together conceptualized as components of a "polycentric" approach to promoting a global culture of cybersecurity. This multi-level, multi-purpose, multi-functional, and multi-sectoral model,[28] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[29] and examining the extent to which national and private control can in some cases coexist with communal management, as may be seen in the success of the largely self-organized Internet Engineering Task Force, the body responsible for the communications side of Internet governance.[30] The field also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action

---

26 *Private International Law*, ORG. AM. ST. (2017), https://perma.cc/JP2M-5RA9.

27 *See, for example*, *Cybersecurity*, HOGAN LOVELLS LLP, https://perma.cc/9FXR-ZXC5; *see* Section II(D), *infra*.

28 Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171–72 (2011).

29 Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, Sept. 2008).

30 For a detailed discussion of early Internet history, see Katie Hafner & Matthew Lyon, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996); *Brief History of the Internet*, INTERNET SOC'Y, https://perma.cc/KT8J-DZA9.

problems"[31] such as cyber attacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[32] Such an approach, in other words, recognizes both the common but differentiated responsibilities of public- and private-sector stakeholders as well as the potential for best practices to be identified and spread organically, generating positive network effects that could, in time, result in the emergence of a cascade toward a positive cyber peace.[33]

The International Telecommunication Union (ITU), a U.N. agency specializing in information and communication technologies, pioneered some of the early work in the field by defining "cyber peace" in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence."[34] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term. That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[35] Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, we can mitigate the risk of cyber war by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[36]

---

31 Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), https://perma.cc/TW2J-CSJQ.

32 Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change,* 9 PERSP. ON POL. 7, 15 (2011). *Cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

33 *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

34 Wegener, *supra* note 18, at 78.

35 The notion of negative peace has been applied in diverse contexts, including civil rights. *See, for example*, Martin Luther King, *Non-Violence and Racial Justice*, CHRISTIAN CENTURY 118, 119 (1957) (arguing "[t]rue peace is not merely the absence of some negative force—tension, confusion or war; it is the presence of some positive force—justice, good will and brotherhood").

36 *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 758, 762 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). For more on this topic, see generally SHACKELFORD, *supra* note 10, at preface. Another related literature that should be explored further stems from the U.S. constitutional law context, including Federalist

The following Section begins the exploration of how we can leverage private international law to promote cyber peace from the bottom up, starting with private-sector cybersecurity innovations that are helping to define a global standard of cybersecurity care including due diligence, cyber risk insurance, project finance, and international arbitration. Next, the movement toward "voluntary" cybersecurity frameworks is analyzed as a data set to begin a more thorough analysis of the current status of customary international cybersecurity law, before turning to bilateral, regional, and global trade and investment treaty frameworks.

B. Cybersecurity Due Diligence

What is cybersecurity due diligence? In the private-sector transactional context, this term has been defined as "the review of the governance, processes and controls that are used to secure information assets,"[37] which makes it stand apart from more outwardly focused public international law concepts of due diligence. This increasingly central concept to a variety of governmental and business activities, as it is used here, builds from this definition and may be understood as the customary national and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and effective governance mechanisms so as to promote cyber peace through enhancing the security of computers, networks, and information and communication technology (ICT) infrastructure. Cybersecurity due diligence obligations may exist between States, between non-State actors (for example, private corporations and end-users), and between State and non-State actors.[38] But determining exactly what nations' due diligence obligations are to secure their networks and to prosecute or extradite cyber attackers is no simple feat. Surprisingly, this central concept has received little attention in the literature.[39]

No. 10, which discusses the extent to which heterogeneous collaboration can mitigate conflict. *See* The Federalist No. 10 (James Madison).

37 Tim Ryan & Leonard Navarro, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks,* KROLL CALL (Jan. 28, 2015), https://perma.cc/W8BB-ZVRA.

38 An earlier version of this research was previously published as Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016).

39 *Cf.* John R. Crook, *Contemporary Practice of the United States Relating to International Law*, 105 AM. J. INT'L L. 775, 795 (2011) ("Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse."); John M. Prescott, *Responses to Five Questions on National Security Law*, 38 WM. MITCHELL L. REV. 1536, 1548 (2012) (discussing the U.S. International Strategy for Cyberspace); Shackelford, *Toward Cyberpeace*, *supra* note 16, at 1354. *See also* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68, 81 (2016) ("[I]nternational law acknowledges that the right of sovereignty and the corresponding duty of due diligence must be in equilibrium. As a matter of law,

This Subsection summarizes the current state of play in this field focusing on relevant International Court of Justice (ICJ) jurisprudence—namely *Corfu Channel*,[40] *Trail Smelter*,[41] and *Nicaragua*[42]—as well as evidence from the private sector to enrich the discussion before moving on to the related topic of cyber risk insurance.

The first relevant ICJ case regarding the due diligence obligations of nations is *Corfu Channel*, particularly the holding in that decision that one country's territory should not be "used for acts that unlawfully harm other States."[43] As applied to cybersecurity (a very different context from its nautical origins), this decision could implicate a duty to terminate cyber emanations from a State's own territory, as well as perhaps a duty to warn other States as to vulnerabilities in its networks that could be exploited by malicious actors and used to harm other nations.[44] Yet this interpretation would be difficult to enforce in practice given the wide array of vulnerabilities replete in a nation's networks, only some of which may be under a nation's direct control, as may be seen by the more than eighty-five percent of U.S. critical infrastructure that is in private hands.[45] Moreover, the growing use of cloud-based services can engender complex jurisdictional issues,[46] while the duty to warn may have itself been subsumed by the 2015 G20 communiqué that called for a duty to assist victim nations,[47] which could implicitly include a duty to warn these nations of impending attacks.

An ad hoc international tribunal also addressed what could become the contours of a cybersecurity due diligence norm in its *Trail Smelter* decision, which centered on pollution crossing the U.S.-Canadian border giving rise to adverse health and environmental effects. The decision, among other things, was concerned about the nature of Westphalian sovereignty, and whether modern notions of sovereignty should be based just on territory, or whether the effects

---

therefore, the due diligence obligation does not require a state to take measures that are beyond its means or otherwise unreasonable.").

40 Corfu Channel (U.K. v. Albania), 1949 I.C.J. 4, ¶ 49 (April 9).

41 Trail Smelter Arbitration (U.S. v. Can.), 3 Rep. Int'l Arb Awards (R.I.A.A.) 1905 (1941).

42 Case Concerning the Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 106-08, 183 (June 27). However, it should be noted that other ICJ jurisprudence is also on point and is not discussed here due to space constraints, including: *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* – General Assembly, ICJ Reports, 8 July 1996, at 22, ¶ 29; *Case Concerning Pulp Mills on the River Uruguay* (Argentina v. Uruguay), Judgment, 20 April 2010, ¶ 193.

43 Corfu Channel, *supra* note 40.

44 Eneken Tikk, *Ten Rules of Behavior for Cyber Security*, 53 SURVIVAL 119, 126 (2011).

45 *See, for example*, STEPHEN FLYNN, THE EDGE OF DISASTER: REBUILDING A RESILIENT NATION 139 (2007).

46 *See, for example*, *Cloudy Jurisdiction: Addressing the thirst for Cloud Data in Domestic Legal Processes*, ELECTRONIC FRONTIER FOUNDATION (Internet Governance Forum-Baku 2012), https://perma.cc/CT7S-8PRD.

47 *See* G20 COMMUNIQUÉ, *supra* note 5.

arising from one nation that impact another could also give rise to obligations through the emerging doctrine of effects jurisdiction.[48] Ultimately, *Trail Smelter* held that "no State has the right to use or permit the use of its territory . . . to cause injury by fume . . . to the territory of another . . . when the case is of serious consequence and the injury is established by clear and convincing evidence."[49] Even though the decision was directed towards the emission of "fumes," *Trail Smelter* has come to represent the broader "no harm" principle, which requires of States "that activities within their jurisdiction or control respect the environment of other States."[50] This "no harm" principle, although directed towards the environment, may enjoy parallels with cyberspace and cybersecurity, and may serve as the foundation for a broader State obligation not to permit domestic activities that result in serious international consequences. Yet it should be noted that this precedent does not yet enjoy widespread State practice, given that it could implicate a huge array of transboundary harms. Still, the reference to "serious consequences" could suggest a graduated cybersecurity due diligence obligation not to permit, for example, harms above a certain threshold, be they environmental or digital.

Finally, the ICJ addressed the core issue of State sovereignty in its *Nicaragua* decision when the Court stated that nations have an obligation not to interfere in one another's domestic affairs if that intervention relates to "the choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[51] This ruling may be read as being in contrast to the Court's effects jurisdiction analysis in *Trail Smelter*. It also tracks the divergent State practice on Internet governance, with some States asserting varying degrees of Internet sovereignty while others profess Internet freedom and the virtues of the "global networked commons."[52] How multi-stakeholder Internet governance may be balanced with classic conceptions of State sovereignty over the long run remains unclear, but the potential for domestic cyber policies to have international ramifications has arguably never been greater;[53] a case in point being the European

---

48 *See, for example*, SIGRUN SKOGLY, BEYOND NATIONAL BORDERS: STATES' HUMAN RIGHTS OBLIGATIONS IN INTERNATIONAL COOPERATION 50 (2006).

49 Trail Smelter Arbitration, *supra* note 41.

50 Ralph Bodle, *Climate Law and Geoengineering*, *in* CLIMATE CHANGE AND THE LAW, IUS GENTIUM: COMPARATIVE PERSPECTIVES ON LAW AND JUSTICE 447, 457–58 (Erkki Hollo et al. eds., 2012).

51 Case Concerning the Military and Paramilitary Activities In and Against Nicaragua, *supra* note 42.

52 *Clinton's Speech on Internet Freedom, January 2010*, COUNCIL ON FOREIGN REL. (Jan. 21, 2010), https://perma.cc/B685-3QSV.

53 *See, for example*, Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd*, 379 F.3d 1120 (9th Cir. 2005), *rev'd en banc*, 433 F.3d 1199 (9th Cir. 2006); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 5 (2006).

Court of Justice's 2015 Safe Harbor decision, which has rippled across cyberspace.[54]

In summary, the international jurisprudence is unsettled, and, as such, is far from dispositive on the question of a cybersecurity due diligence norm. Both State practice and lessons from the private sector can and should be considered to help build out the private international law of cyber peace, which thus far has been largely untapped to answer such questions. For example, facets of national cybersecurity strategies could, in time, crystallize into customary international law as State practice clarifies.[55] Similarly, given the extensive public-private cross-pollination of cybersecurity best practices, private-sector efforts aimed at enhancing cybersecurity are informative given the extent to which they are shaping national policymaking, with the 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework being a case in point.[56]

Jason Weinstein, former deputy assistant attorney general at the U.S. Department of Justice, summarized the issue of cybersecurity due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data-security problems."[57] In other words, "[c]yber risk should be considered right along with financial and legal due diligence considerations."[58] Already a majority of respondents in one 2014 survey reported that cybersecurity challenges are altering the M&A landscape, while eighty-two percent said that cyber risk would become more predominant over the following eighteen months.[59] Simply put, according to Thomas J. Smedinghoff, of counsel at Locke Lord Edwards LLP, "The cybersecurity situation of the company you are acquiring affects the value of the company, it affects the liability you might be taking on, and it affects the costs you might have to incur."[60] Managers now considering what form cybersecurity due diligence should take have a wealth of

---

54 *See* Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact With U.S. Violates Privacy*, WALL ST. J. (Oct. 6, 2015), https://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361; Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, SETON HALL J. DIPL. & INT'L REL. (forthcoming 2017) (discussing the case in some detail).

55 *See* Jean-Marie Henckaerts & Louise Doswald-Beck, *Assessment of Customary International Law*, INT'L COMM. RED CROSS (2005), https://perma.cc/SH46-EVFM.

56 *See Update on the Cybersecurity Framework*, NIST (Dec. 5, 2014), https://perma.cc/2FKE-RM2W.

57 Rachel Ensign, *Cybersecurity Due Diligence Key in M&A Deals*, WALL ST. J. (Apr. 24, 2014), http://blogs.wsj.com/riskandcompliance/2014/04/24/cybersecurity-due-diligence-key-in-ma-deals/.

58 Erin Ayres, *Cybersecurity Easing its Way into M&A Due Diligence*, ADVISEN (Aug. 22, 2014), https://perma.cc/W27L-4TLE.

59 *Id.*

60 Michael Greene, *M&A Due Diligence Must Include Cybersecurity Analysis, Attorneys Say*, BNA (May 20, 2015), https://perma.cc/ZA5D-55SG.

resources (as well as a growing array of compliance obligations) to consider.[61] These include, in the U.S. context, the NIST Cybersecurity Framework discussed further below,[62] as well as guidance from the Securities and Exchange Commission, National Association of Corporate Directors, and the Payment Card Industry (PCI) Security Standards Council.[63] Together, these frameworks, and others, provide the beginnings of a cybersecurity due diligence standard guiding judges as they work through causes of action such as breach of fiduciary duty and negligence resulting from data breaches.[64]

Despite some progress, though, many remain predominantly reactive in their cybersecurity stances.[65] In order to improve the status quo, firms must leverage proactive cybersecurity best practices ranging from risk-based data management to minimizing the danger of insider threats through meshing corporate and human resources policies and reviewing the cybersecurity track records of vendors and potential partners.[66] Over time, as legal harmonization progresses, there will be more opportunities to build out cybersecurity norms, including due diligence, which is already being assisted by the rapid growth and sophistication of the cyber risk insurance market.

C. Cyber Risk Insurance

Insurance has been called a "key part of the [cybersecurity] solution," but it has only recently begun to catch on, albeit in fits and starts.[67] After all, insurance is a primary way that we as a society manage risky behavior across myriad sectors, from car accidents to healthcare. Indeed, state and federal law even requires the purchasing of different types of insurance to mitigate risk—including car and health insurance—which begs the question, why not cyber risk insurance? The trouble, as we will see, lies in the accurate assessment of risk. Still, as data models and frameworks improve, such policies are increasingly popular tools for a growing array of small- and medium-sized enterprises as well as multinational

---

61 *See* Stone v. Ritter*,* 911 A.2d 362, 370 (Del. 2006).

62 *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2014), https://perma.cc/H924-X77W.

63 *See* Ayres, *supra* note 58.

64 *Cf.* Willingham v. Global Payment, 2013 WL 440702 at *19 (N.D. Ga. Feb. 5, 2013) (reflecting an alternative view in which courts are reluctant rely on data security standards as a means of determine whether a duty was owed).

65 *See* MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://perma.cc/X38C-DRDP.

66 For more on this topic, see generally Amanda N. Craig, Scott J. Shackelford, & Janine Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

67 Interview with Chris Palmer, Google engineer and former technology director, Electronic Frontiers Foundation, in San Francisco, Cal. (Feb. 25, 2011).

corporations and major universities. Even the U.S. government has begun to discuss ways in which to encourage the more rapid update of cyber risk insurance policies.[68] Indeed, according to Roger Smith of Allianz, "Cyber insurance is probably the fastest growing insurance in the world."[69] This Subsection discusses the triumphs and travails of the cyber risk insurance market before moving on to related due diligence considerations.

Insurance firms have been experimenting with cyber risk insurance policies for more than a decade; Zurich North America, for example, began offering "a reward for information leading to the conviction of" cyber terrorists back in 2002.[70] By some estimates the market will be worth more than $7.5 billion by 2020 with an increasing number of firms looking to invest in coverage,[71] a trend that could be reinforced depending on regulatory developments such as the Securities and Exchange Commission (SEC) cyber attack disclosure guidelines.[72] Other nations are going further, with Australia requiring cyber attack disclosure in 2016,[73] which could better inform the process of quantifying risk premiums. As one 2008 survey explained, "cyber insurance is a concept that has a great deal of intellectual appeal, has seen a degree of implementation, but that isn't taking the enterprise world by storm."[74] Part of the reason is cost.[75] While some small firms like Brookeland Fresh Water Supply in East Texas, from which cybercriminals stole $35,000, have been kept afloat by insurance (because of its insurance policy,

---

68 *See* SANS Institute, WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 24 (2003), https://perma.cc/P6L8-CUZ9; Cybersecurity Act of 2009, S. 773, 111th Cong. § 15(1), (2009) (providing for the creation of "a market for cybersecurity risk management, including the creation of a system of civil liability and insurance (including government reinsurance)").

69 Emily Stewart, *Cyber Attack Insurance Growing Fast*, ABC (Oct. 9, 2015), https://perma.cc/CW2W-UW3E.

70 Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), https://perma.cc/U4F6-YB92; *see* Press Release, Hiscox, Safeonline Launches Internet Security Insurance, https://perma.cc/AV5J-MWLQ.

71 *See* Jim Finkle, *Cyber Insurance Premiums Rocket After High-Profile Attacks*, REUTERS (Oct. 12, 2015), https://perma.cc/6AVX-GPL9; Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES BITS (Dec. 29, 2011), https://perma.cc/Q4B8-DW6F.; Robert Lemos, *Should SMBs Invest in Cyber Risk Insurance?*, DARK READING (Sept. 9, 2010), https://perma.cc/HXU2-7LPZ.

72 *See* Perlroth, *supra* note 71.

73 Stewart, *supra* note 69.

74 Robert Richardson, *CSI Computer Crime & Security Survey* at 11 (2008), https://perma.cc/PH8H-3JLJ.

75 *See* Lemos, *supra* note 71; *see also Travelers Adds Cyber Protection Tailored to Small Businesses*, INS. J. (Jan. 22, 2013), https://perma.cc/SA75-U76X. DHS summarized the current state of cyber risk insurance in 2012, noting that "[w]hile a sizable third-party market exists to cover losses suffered by a company's customers, first-party policies that address direct harms to companies themselves remain expensive, rare, and largely unattractive." DHS, CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT 1 (2012), https://perma.cc/L2QE-L4BC; Nathan Brown, *The Costs of Having (and NOT Having) Cyber Insurance*, NEXTECH (Mar. 31, 2015), https://perma.cc/STX2-28LX.

instead of going out of business, it only lost its $500 deductible), many other small, medium, and large enterprises have been refused coverage.[76] If managers are not forthcoming, or do not have adequate safeguards in place, then the insurance company may decline coverage, as happened to British electrical grid operators in early 2014.[77] And since cyber attacks can happen irregularly, the cost of protection may not always be worth it,[78] especially given the need for applicant firms to pass the equivalent of a cybersecurity audit.[79]

Calculating cyber risk insurance premiums is no simple matter; there is little reliable data—a factor that is critical,[80] for example, to pricing healthcare and automobile insurance. Still, many firms are moving forward despite the relative newness of the problem and the relative lack of incentives for effective information sharing, which can result in skewed calculations.[81] This is notwithstanding the fact that annual premiums can run from the thousands to the hundreds of thousands depending on the type and size of organization seeking coverage.[82] Geography matters in the number of insurance options that firms have—Australian companies, for example, can reportedly choose from fifteen carriers,[83] whereas there are more than twenty providers in the U.S. depending on the specific market in question.[84] And there is evidence that deductibles are rising in step with proliferating cyber risk with some firms reportedly limiting their total coverage to $100 million.[85] Healthcare companies and retailers in particular—with both sectors having experienced recent high-profile breaches, such as Anthem and Target—are experiencing some of the steepest rises, with some firms facing a

---

76 *See The Case for Cybersecurity Insurance, Part II*, KREBS ON SEC. (Jul. 10, 2010), https://perma.cc/994Q-XBLN; *see also* Tony Morbin, *Should You Use Cyber Insurance to Mitigate Risk?*, SC MEDIA (Aug. 20, 2014), https://perma.cc/9EF5-SDKA.

77 *See* Mark Ward, *Energy Firm Cyber-Defense is 'Too Weak', Insurers Say*, BBC (Feb. 26, 2014), https://perma.cc/93XK-TESE.

78 *Cf.* Denise Dubie, *Corporate Security Spending Not in Line with Real-World Requirements*, NETWORK WORLD (May 2003), https://perma.cc/6U69-ATJN. *But see* Riva Richmond, *How to Determine If Cyber Insurance Coverage Is Right for You*, ENTREPENEUR (June 5, 2012), https://perma.cc/8EJS-MES6; Morbin, *supra* note 76.

79 *See, for example*, Brooke Yates & Katie Varholak, *Cyber Risk Insurance - Navigating the Application Process*, SHERMAN & HOWARD (June 6, 2013), https://perma.cc/6BM2-VCN9.

80 *But see* Sarah Veysey, *Insurers Urge Anonymous Database to Help Underwrite Cyber Risks*, BUS. INS. (May 23, 2016), https://perma.cc/EBE8-9SJP ("The Association of British Insurers has called for a national anonymous database of cyber incidents to enable the insurance market to better assess, underwrite and price cyber risks.").

81 *See* DHS, *supra* note 75, at 1.

82 Stewart, *supra* note 69.

83 *Id.*

84 *See, for example*, CYBER INSURANCE: A LAST LINE OF DEFENSE WHEN TECHNOLOGY FAILS, LATHAM & WATKINS CLIENT ALERT 1675, at 1 (Apr. 15, 2014), https://perma.cc/C7RA-RZJS.

85 *See* Finkle, *supra* note 71.

tripling of costs.[86] Anthem, for example, had to agree to pay the first $25 million of future breach costs out of pocket before it could get insured for $100 million in coverage.[87] Target reportedly was hoping to cover $90 million of the $264 million in losses from its 2014 breach through insurance.[88] Some discounts are available, though, to help with spiraling costs; Bryce and AIG, for example, have a history of offering rebates for firms using secure hardware and software packages.[89] Other insurers are going further. Ben Beeson of Lockton Companies, for example, has stated that, "Insurers are promoting newer technologies for securing payment card transactions that exceed credit card companies' requirements, such as tokenization and end-to-end encryption."[90] Over time, such efforts could help ratchet up the overall level of cybersecurity preparedness across a range of businesses. And there is plenty of room to grow with an array of industries, such as manufacturing, as well as the public sector, largely lacking coverage.[91] Still, there is an active debate underway about the utility of incentivizing the purchase of cyber risk insurance given that it could lead to moral hazard by contributing to a more reactive mindset on the part of managers, meaning that it should only be considered as one piece in a polycentric approach aimed at managing cyber risk.

D. Project Finance and International Arbitration

Many leading global law firms include project finance practice groups that help arrange financing for large infrastructure projects around the world. To take one example, Hogan Lovells LLP has been involved with deals ranging from defense and healthcare to light rail, sanitation, and satellites, in deals totaling more than $250 billion as of 2016.[92] Cybersecurity is forming an increasingly important component of these deals. This trend has been recognized by such groups as the Financial Industry Regulatory Authority (FINRA), which noted in a 2015 report that, "[b]roker-dealers are increasingly exposed to cybersecurity risks, and breaches at a broker-dealer could entail adverse implications for investors, firms, capital markets and even broader swaths of the financial system."[93] Ensuring that

---

86 *See id.*

87 *Id.*

88 *Id.*

89 *See* DHS, *supra* note 75, at 1.

90 Finkle, *supra* note 71.

91 *See* Caitlin Bronson, *The 5 US Industries Most Uninsured Against Cyber Risk*, INS. BUS. AM. (Oct. 12, 2015), https://perma.cc/Z3E5-2JW4; Matt Williams, *Why Most Governments Don't Carry Cyber Insurance*, GOVT. TECH. (Aug. 7, 2013), https://perma.cc/YY7A-UTAY.

92 *See Infrastructure, Energy, Resources, and Projects*, HOGAN LOVELLS, https://perma.cc/A9EQ-CFX8.

93 *FINRA Issues Report on Cybersecurity Practices, Cybersecurity Investor Alert*, FINRA (Feb. 3, 2015), https://perma.cc/LE5Z-3H8L.

a robust set of cybersecurity best practices is in place across the financial industry and within law firms (which are themselves often the targets of cyber attackers[94]) can do a great deal to help mitigate cyber risk.

When project finance deals go awry, or nations pass policies or even expropriate investments, international dispute resolution proceedings including arbitration may result, which are fast becoming another major (if somewhat controversial[95]) component of many firms international practice groups. One particular facet of this practice that is increasingly of interest in the cybersecurity context is the rise of investment treaty arbitration under bilateral investment treaties (BITs), which are discussed further below.[96] In short, investment treaty arbitration is a treaty-based regime that leverages the rules and structures of international law along with private arbitration to make binding decrees on governments regarding the regulatory relationship between investors and the State.[97] Myriad forums exist for investment-treaty arbitration, but among the most important is the International Convention for the Settlement of Investment Disputes (ICSID). This specific arbitral process is important since it is designed to overcome the adjudicatory problems that often arise when a sovereign is involved in an international commercial transaction. The ICSID process is supposed to be autonomous, so much so that contracting States cannot even entertain challenges to ICSID awards. In practical effect, the only power a national court retains over ICSID judgments is the ability to recognize and enforce the ICSID award itself, subject to the ICSID internal appeal procedure created within the ICSID framework.

As of April 2016, the ICSID Convention has been ratified by 161 States,[98] yet it suffers from an underwhelming number of submitted cases.[99] Some commentators, such as noted arbitration authority Professor Thomas Carbonneau, highlight the problems associated with enforcement as one of the

---

94 *See* Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://perma.cc/NJS5-CVTK.

95 For example, concerns have long centered on limitations to national sovereignty, with critics arguing "that the process should be more fully transparent and open to participation by concerned citizens, given the public importance of the issues at stake in many of the cases." ANTHONY R. PARRA, THE HISTORY OF ICSID 238 (2012) (arguing that "Other influential voices were raised to argue that investment treaties and arbitration could unduly constrain governments from introducing much needed reforms, including those concerning human rights.").

96 *See* Section II(F), *infra*.

97 For more on this topic, see Shackelford et al., *Using BITs to Protect Bytes*, *supra* note 16 (representing the first publication of parts of this analysis).

98 International Centre for Settlement of Investment Disputes (ICSID), *List of Contracting States and Other Signatories of the Convention (as of April 12, 2016)*, https://perma.cc/XF4M-DJT5.

99 *See* International Centre for Settlement of Investment Disputes (ICSID), *The ICSID Caseload – Statistics*: *Issue 2016-1* at 7–9, https://perma.cc/AT6Q-DAB4.

main obstacles to wider use of the ICSID Convention.[100] The ability of a state to essentially renege on its promise to arbitrate and enforce an award is a troubling aspect of the ICSID process, a concern that is further compounded by the traditional confidentiality of arbitration proceedings and awards. Indeed, beyond investment disputes, international commercial arbitration is a closed—almost secret—process. Shrouded behind a curtain of confidentiality (so sacrosanct that some national courts have inserted confidentiality into an otherwise silent arbitration agreement[101]), the end result is that international arbitration has limited precedential value in building a law of cyber peace. For example, a search of the Investor-State Law Guide—a leading resource for international arbitral decisions—conducted in October 2015 for various key terms referencing cybersecurity only resulted in a single result for the prefix "cyber." This 2015 case, *Lao Holdings*, did not deal with cybersecurity per se, but rather related areas such as "cyber gossip."[102] Other arbitral decisions may well have referenced cybersecurity as of this writing, but the fact that many are kept confidential means that their precedential value is quite limited.

E. The Rise of "Voluntary" Cybersecurity Frameworks

At the next level up from private-sector innovation in the due diligence, insurance, project finance, and arbitration arenas, States are also experimenting with a wide array of frameworks and other bottom-up cybersecurity governance efforts aimed at securing critical infrastructure, protecting trade secrets, and mitigating the risk of cyber conflict.[103] Among other arenas, this trend may be seen in an increasing array of nations, including the U.S.,[104] creating voluntary cybersecurity frameworks designed to help foster a culture of cybersecurity

---

100 *See* THOMAS CARBONNEAU, CASES AND MATERIALS ON THE LAW AND PRACTICE OF ARBITRATION 911–13 (2003).

101 For example, the English courts have previously made such a declaration. *See* Anjanette H Raymond, *Confidentiality, in a Forum of Last Resort? Is the Use of Confidential Arbitration a Good Idea for Business and Society?*, 16 AM. REV. INT'L ARB. 479 (2005) (discussing the English case of City of Moscow v. Bankers Trust, [2004] All ER (D) 62 (Jan)).

102 *See* Lao Holdings N.V. & The Government of the Lao People's Democratic Republic, Discussion on the Merits (June 10, 2015), at 40, ICSID Case No. ARB (AF)/12/6.

103 *See, for example*, Matthew Braga, *Canada Doesn't Know How to Regulate Cyber Weapons Sales*, MOTHERBOARD (Sept. 8, 2014), https://perma.cc/5JMY-9PPR.

104 *See, for example*, Paul Rosenzweig, *The Unpersuasiveness of the Case for Cybersecurity Regulation – An Introduction*, LAWFARE (May 17, 2012), https://perma.cc/N67K-XFWW; Michael Daniel, *Assessing Cybersecurity Regulations*, WHITE HOUSE (May 22, 2014), https://perma.cc/VB7N-BML3 ("The major outcome is that the Administration's analysis supports our current voluntary approach to address cyber risk.").

particularly among critical infrastructure providers.[105] This effort, led by NIST,[106] is breaking new ground when it comes to fashioning a standard of cybersecurity care that is already having an impact not only in the U.S., but around the world with NIST actively collaborating with several dozen nations. It may indeed be true that none of these nations have gotten the regulatory mix exactly right given the continuing prevalence of cyber attacks across them,[107] but it is equally accurate that learning can and does happen across nations and sectors that could lead to what Professors Jack Goldsmith and Tim Wu call "regulatory spillover effects," which can "be good or bad, depending on which regulatory scheme prevails."[108] As such, it is important not to ignore State practice when it comes to building out the law of cyber peace. Space constraints prohibit a thorough recounting of all the relevant available data.[109] However, in summary, these nations and the E.U. generally (out of the more than twenty with which NIST has had active consultations) are, to a greater or lesser extent, emulating various aspects of the NIST Cybersecurity Framework in their domestic policymaking. The U.K., Italy, Japan, and, to a lesser extent, Australia seem to be the most supportive of many aspects of the NIST Cybersecurity Framework, as is the E.U., as seen in its support of core NIST Cybersecurity Framework terminology. In contrast, South Korea's philosophy of more top-down cybersecurity policymaking stands in contrast to the spirit of bottom-up cybersecurity governance, even as it engages with the U.S. on NIST Cybersecurity Framework deployment. Such State practice is informative in discussions relating to cybersecurity norm development, a topic unpacked further in Section IV.

At the next conceptual level up from domestic policymaking, it is also important to note the role played by national cybersecurity strategies in laying out how nations view both the cybersecurity challenge and the role of the State in meeting it.[110] For example, in an analysis of thirty-four national cybersecurity strategies undertaken in 2015, it was found that fifty-six percent of the nations

---

105 Other nations, though, are taking myriad other approaches. Israel, for example, has created a National Cyber Bureau to aid in standards setting. *See, for example*, Daniel Benoliel, *Towards a Cyber Security Policy Model: Israel National Cyber Bureau (INCB) Case Study* (Univ. of Haifa Discussion Paper, July 2014), https://perma.cc/85AK-8BX9.

106 *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK at i (2014), https://perma.cc/H924-X77W.

107 *See, for example*, Kaspersky Cybermap, https://cybermap.kaspersky.com/ (last visited April 5, 2017).

108 Jack Goldsmith, *Response to Paul on Cyber-Regulation for Critical Infrastructure*, LAWFARE (May 21, 2012), https://perma.cc/EHC3-A4V9.

109 For more on this topic, see Shackelford, Russell, & Haut, *supra* note 16; ITU, GLOBAL CYBERSECURITY INDEX & CYBER WELLNESS PROFILES 1 (2015), https://perma.cc/K6LA-RH5Y (ranking nations in terms of their vulnerability to and mitigation strategies for cyber attacks).

110 For more on this topic, see Shackelford & Kastelic, *supra* note 16.

surveyed referenced the importance of information sharing as a key component of managing the multifaceted cyber threats to critical infrastructure, whereas only twenty-four percent mentioned the need for new regulation to enhance critical infrastructure cybersecurity.[111] These data help illustrate the extent to which there is a reticence on the part of a number of nations about taking a too heavy-handed role when it comes to regulating cybersecurity, highlighting the attractiveness of a more bottoms-up NIST Cybersecurity Framework-like approach.

Still, it remains unclear exactly how many nations will follow the lead of these countries in preferring a bottoms-up approach to cybersecurity risk management. Indeed, some of the leading cyber powers—including China and Russia—favor more State-centric approaches to enhancing critical infrastructure cybersecurity. This may be seen in the Russian government's stated goal of by 2020 centralizing its efforts to detect and prevent cyber attacks, including those on critical infrastructure, giving over many functions to the Federal Security Service (FSB).[112] Moreover, regime effectiveness studies are notoriously difficult to undertake in this context. For example, the U.S. has more than 3,200 independent power utilities, unlike, for example, Germany, which has four major providers.[113] Some U.S. firms are taking appropriate steps to secure their systems, but differences in resources and expertise make the uptake of best practices haphazard in a purely bottoms-up system,[114] even as more space for experimentation and innovation is possible with so many actors identifying and instilling best practices.[115] Thus, as State practice crystallizes further, and by mining data such as has begun to be gathered by the International Telecommunication Union,[116] further research is required to better understand the most effective role for States in furthering a customary law of cyber peace.

F. Bilateral Investment Treaties

Beyond State practice, there is an increasingly important role being played by minilateral legal instruments in promoting especially bilateral cybersecurity, though realizing the full benefit of these instruments will require reform as is

---

111 *See id.* at 913–14.

112 *See Russia has Developed a National Cyber Security Policy*, FISMA NEWS, https://perma.cc/K22V-6LV2.

113 *See* U.S. DEP'T ENERGY, A PRIMER ON ELECTRIC UTILITIES, DEREGULATION, AND RESTRUCTURING OF U.S. ELECTRICITY MARKETS v. 2.0, at 2.1 (May 2002); CHRISTIAN SCHÜLKE, THE EU'S MAJOR ELECTRICITY AND GAS UTILITIES SINCE MARKET LIBERALIZATION 130 (2010).

114 *See* Letter from Michael Assante, NERC Vice President and Chief Security Officer, to Industry Stakeholders (Apr. 7, 2009), https://perma.cc/H437-PHJE (discussing designating critical cyber assets).

115 For more on the methodological challenges of undertaking cybersecurity regime effectiveness studies, see SHACKELFORD, *supra* note 10, at 312–66.

116 *See* GLOBAL CYBERSECURITY INDEX, *supra* note 109.

discussed below. Before delving into the role of BITs in potentially protecting bytes, though, it is first important to offer some context. During the colonial era up to the nineteenth century, the leading developed nations held the view that foreign investors were entitled to property rights protections under international law, and that if their property was in fact taken then they were entitled to "prompt, adequate, and effective compensation."[117] The modern terminology to describe such expropriations arose in the 1930s in a dispute between the governments of Mexico and the U.S. involving confiscated agrarian and oil properties, some of which were owned by U.S. citizens, resulting in a now famous diplomatic exchange between U.S. Secretary of State Cordell Hull and the Mexican Minister of Foreign Affairs.[118] In one of Hull's notes, he put forward a standard for compensation that became the leading formulation for the protection of investor property rights under customary international law through the 1970s: "no government is entitled to expropriate private property, for whatever purpose, without provision for prompt, adequate, and effective payment therefore."[119] Gradually, though, with the colonial era ending, new legal insturments began to take the place of the Hull Rule, namely the rise of BITs that have, over time, become the most important legal mechanism for the encouragement and governance of foreign direct investment (FDI) and, increasingly, trade secret protections.

BITs accord wide-ranging rights to investors, including the protection of contractual rights, and recourse to international arbitration should any disputes arise,[120] a topic of increasing political sensitivity both in Europe and the U.S.[121] The driving force behind this facet of international law has been the rapid growth of FDI, which, according to the World Bank, "increased seven fold from . . . 1970 to 2000."[122] By 2012, FDI stocks had risen to some $22 trillion.[123] These growing

---

117 Frank G. Dawson & Burns H. Weston, "*Prompt, Adequate and Effective" A Universal Standard of Compensation?*, 30 FORDHAM L. REV. 727, 734 (1962); *see also* Case Concerning the Factory at Chorzow (Ger. v. Pol.), 1926-29 P.C.I.J. (ser. A), Nos. 7, 9, 17, 19, *excerpted in* HENRY J. STEINER ET AL., TRANSNATIONAL LEGAL PROBLEMS 451–54 (1994).

118 Notes exchanged between the U.S. and Mexico during the 1938 disputes are reprinted in 3 GREEN H. HACKWORTH, DIGEST OF INTERNATIONAL LAW § 228, at 655–65 (1942); *see* Andrew Guzman, *International Law: A Compliance Based Theory*, 90 CAL. L. REV. 1823, 1823–25 (2002).

119 RONALD CHARLES WOLF, TRADE, AID, AND ARBITRATE: THE GLOBALIZATION OF WESTERN LAW 26 (2004).

120 *See* Zachary Elkins, Andrew T. Guzman, & Beth A. Simmons, *Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960-2000*, 2008 U. ILL. L. REV. 265, 268–69 (2008).

121 *See, for example*, THOMAS E. CARBONNEAU, CARBONNEAU ON INTERNATIONAL ARBITRATION: COLLECTED ESSAYS 126 (2011).

122 Elkins, *supra* note 120, at 266.

123 Daniel Ikenson, *Policymakers Must Remove The Barriers To Foreign Investment In The United States*, FORBES (Oct. 30, 2013), https://perma.cc/457E-DKLJ.

figures have fueled the rise of BITs, which numbered nearly 3,000 by 2013[124] and covered a large range of industry sectors and business activities.[125] At the July 2013 China-U.S. Strategic and Economic Dialogue, for example, the U.S. and China publicized plans to begin negotiating an expansive BIT that will reportedly include the difficult issue of enhancing bilateral cybersecurity.[126] According to U.S. Treasury Secretary Jacob J. Lew, if successful, this would be "the first time China has agreed to negotiate a bilateral investment treaty, to include all sectors and stages of investment, with another country."[127] Although some questions already have arisen regarding the seriousness of both sides in the negotiations, with direct investment between China and the U.S. increasing and trade secrets theft showing few signs of abating,[128] the potential for significant progress that could help deepen the U.S.-Chinese cybersecurity dialogue exists.[129] Indeed, it may already be bearing some fruit with the U.S.-China "cyber accord" in September 2015 that included measures to fight intellecutal property theft.[130]

In the U.S., trade secret theft of a product in interstate or international commerce violates the Economic Espionage Act[131] if "the intended beneficiary is a foreign power."[132] However, the utility of the Economic Espionage Act in prosecuting trade secret theft is limited in the context of foreign state-sponsored cyber attacks that target corporate trade secrets, given the difficulties of attribution, extradition, and determining an appropriate forum to resolve the dispute—hence the potential value of investor-state arbitration. Other applicable U.S. statutes include the Computer Fraud and Abuse Act,[133] the National Stolen Property Act,[134] wire fraud,[135] and the 2016 Defend Trade Secrets Act, which created a federal cause of action for trade secret misappropriation.[136]

---

124 UNCTAD, WORLD INVESTMENT REPORT 101 (2013).

125 *See* GUS VAN HARTEN, INVESTMENT TREATY ARBITRATION AND PUBLIC LAW 171 (2007).

126 *See* Annie Lowrey, *U.S. and China to Discuss Investment Treaty, but Cybersecurity Is a Concern*, N.Y. TIMES (July 12, 2013), http://www.nytimes.com/2013/07/12/world/asia/us-and-china-to-discuss-investment-treaty-but-cybersecurity-is-a-concern.html.

127 *Id.*

128 *See, for example*, Chen Weihua, *US, China Hopeful of BIT After Talks Reignited*, CHINA DAILY (July 13, 2013), https://perma.cc/5CG6-JQVZ.

129 *See China Plans First Talks With U.S. Under Cybersecurity Dialogue*, BLOOMBERG (July 5, 2013), https://perma.cc/2LG7-9EUK.

130 *See, for example*, Everett Rosenfeld, *US-China Agree to Not Conduct Cybertheft of Intellectual Property*, CNBC (Sept. 25, 2015), https://perma.cc/KZ9B-ASL9.

131 18 U.S.C. § 1832.

132 *See* Charles Doyle, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, CRS Report R42682 (2016), https://perma.cc/967C-LWFD.

133 18 U.S.C. §§ 1030(a)(4), (e)(2).

134 18 U.S.C. § 2314.

135 18 U.S.C. § 1343.

136 Pub. L. No. 114-153 (May 11, 2016).

The world's various legal systems and cultures maintain different levels of intellectual property protections. Therefore, as emphasized by U.S. Deputy Secretary of State William Burns, the U.S. and China, for example, "need to reach a shared understanding of the rules of the road"[137] in cyberspace. BITs may be a vehicle to engender such norms. The use of BITs in this manner provides two key elements often lacking in other protective regimes like the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS): grievances that fall within the purview of a BIT not only can be pursued by an individual but also can be resolved within an internationally-accepted arbitration mechanism. The use of arbitration provides several advantages, as has been mentioned, such as the use of a neutral setting for resolution of grievances, well-established rules of arbitration and enforcement of awards, and access to and the use of well-established investor-dispute focused arbitration institutions. And of course, pursuing a claim under a BIT agreement allows a foreign investor to bring a claim against that host state in investor-state arbitration without the need to petition its home government to initiate dispute settlement proceedings.[138]

Despite its advantages, BIT-based investment arbitration is not without its detractors. Unlike its predecessor—the Treaty of Friendship, Commerce and Navigation discussed in Section III—BITs are designed to be less complicated and more narrowly focused. However, they also are prone to unpredictable and, at times, even inconsistent interpretation. Their brevity created an apparent justification for judicial activism in order to clarify vague treaty language and to close gaps left open by the drafters.[139] As a result of this and other concerns, states have begun reconsidering their approach to investment treaties. As some countries started to denounce their BITs, others, like Bolivia and Ecuador, exited the ICSID Convention altogether.[140] In fact, States became more hesitant to negotiate BITs.[141] This relative decline in BIT enactment and participation rates cannot be explained by a saturation of the field alone.[142] Rather, more and more countries have put their BIT programs on hold in order to re-evaluate their approach to investment policymaking. These statistics highlight the ambiguity with which many nations view BITs and investor-state arbitration, with BIT rates

---

137 *See* Paul Eckert & Anna Yukhananov, *U.S., China Agree to Restart Investment Treaty Talks*, REUTERS (July 12, 2013), https://perma.cc/2MDR-2PA8.

138 *See* Gaetan Verhoosel, *The Use of Investor-State Arbitration Under Bilateral Investment Treaties to Seek Relief for Breaches of WTO Law*, 6 J. INT'L ECON. L. 493, 495 (2003).

139 *See* Wolfgang Alschner, *Interpreting Investment Treaties as Incomplete Contracts: Lessons from Contract Theory*, (SSRN ID No. 2241652, Mar. 31 2013), https://perma.cc/A3M3-GMA6.

140 UNCTAD, Denunciation of the ICSID Convention and BITS: Impact on Investor-State Claims, IIA Issues Note, No. 2, 2010, UNCTAD/WEB/DIAE/IA/2010/6.

141 UNCTAD, WORLD INVESTMENT REPORT 2012: TOWARDS A NEW GENERATION OF INVESTMENT POLICIES, UNCTAD/WIR/2012 at 84 (2012).

142 *See* UNCTAD, WORLD INVESTMENT REPORT 2011: NON-EQUITY MODES OF INTERNATIONAL PRODUCTION AND DEVELOPMENT, UNCTAD/WIR/2011 at 102–03 (2011).

dropping and some power centers pushing back on the use of arbitration, even as the overall number of BITs and arbitrations continues to increase.

Ultimately, for BITs to realize their potential as an important component of the law of cyber peace, the political and legal costs of these agreements need to be mitigated and interest rekindled on the part of developed and developing nations alike. Greater attention will also need to be paid to the compensation standard in play, since compulsory licenses will likely not fully compensate those that have lost trade secrets. Further, more transparency is needed in the investor-state arbitration arena to help address legal fragmentation and build the precedent necessary for stable and predictable international customary cybersecurity law. The absence of transparency is a growing concern in the international community as investor-state arbitration rates increase, but there have been positive steps made in this regard that should be reinforced in future BITs.

G. World Trade Organization

Aside from BITs, cybersecurity is also becoming an important topic in regional and global trade negotiations. Ongoing U.S.-E.U. trade talks have been shaped in part by cybersecurity and privacy concerns, especially in the aftermath of NSA surveillance programs and intellectual property protections.[143] The proposed Trans-Pacific Partnership also has a cybersecurity component (which may still move forward without immediate U.S. participation),[144] and even the World Trade Organization (WTO) employs enforcement mechanisms that may be applicable to cyberattacks if national security concerns could be overcome.[145] Together, these multilateral investment and trade regimes could provide a basis for fostering regional collaboration to enhance global cybersecurity at a time of relatively slow progress on domestic and multilateral cybersecurity

---

143 *See, for example*, Doug Palmer, *U.S. EU Launch Free Trade Talks Despite Spying Concerns*, INS. J. (July 9, 2013), https://perma.cc/Z3DF-HQBM. *But see* James Fontanella-Khan, *Data Protection Ruled Out of EU-US Trade Talks,* FIN. TIMES (Nov. 4, 2013), https://perma.cc/A3BP-8DP2 ("Brussels has ruled out a German push to include data protection rules in a proposed EU-US free trade pact.").

144 *See* Kevin Collier, *Sen. Ron Wyden on the Problems with the Trans-Pacific Partnership*, DAILY DOT (Sept. 19, 2012), https://perma.cc/6Q9L-SA8Q; *New Zealand, Australia Leaders Press for TPP to Move Forward*, BRIDGES (Feb. 23, 2017), https://perma.cc/4C85-AV4Y.

145 However, regarding the latter, while the WTO has been used as a forum to air broader concerns among the Member States, it has to date been a factor in the cybersecurity context because of provisions allowing nations to shirk their free trade commitments when they conflict with national security. *See, for example*, Allan A. Friedman, *Cybersecurity and Trade: National Policies, Global and Local Consequences*, CTR. FOR TECH. INNOVATION AT BROOKINGS 10–11 (2013), https://perma.cc/LD4M-ZFPV; James A. Lewis, *Conflict and Negotiation in Cyberspace*, CTR. STRATEGIC & INT'L STUD. at 48–51 (2013), https://perma.cc/552F-5MK2.

policymaking.[146] Yet the applicability of these regimes to cybersecurity has been underappreciated in the literature to date,[147] in part because of legitimate concerns about the utility of this field of law as applied to cybersecurity that requires clarification and reform, as is discussed further below. Specifically, this Subsection builds from the foregoing discussion of BITs to ascertain the applicability of multilateral trade forums—notably the WTO—in helping to foster a law of cyber peace.

Beginning in 1994, the WTO expanded its coverage from trade in goods and trade in services to coverage of intellectual property through TRIPS.[148] Article 39 of this Agreement references trade secrets, which could be invaluable to negatively impacted individuals and firms that have been the victims of intellectual property theft.[149] As members of the WTO, both the U.S. and China, along with other important cyber powers such as Russia, are bound by the trade secret standards mandated by TRIPS.[150] Yet criticism of TRIPS has continued as applied to trade secrets; for example, some have argued that TRIPS has too limited coverage and an inadequate compensation regime. Similarly, even though States often comply with WTO judgments,[151] it has "no jailhouse, no bail bondsmen, no blue helmets, no truncheons or tear gas." [152] In other words, enforcement continues to be problematic, leaving the utility of this vehicle to help address the plight of victims in cross-border transactions involving trade secrets theft uncertain. More generally, the WTO has to date been ineffective as a forum for enhancing global cybersecurity because of the aforementioned national security exception. BITs may also be hobbled by the same exception unless perhaps the "good faith" standard put forward by the U.S. catches on and is made more robust.[153] Ultimately, however, both bottom-up (e.g., BITs) and top-down (e.g., WTO) regimes have unique benefits and drawbacks, necessitating a polycentric approach

---

146 *See, for example*, Scott Shackelford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 111 (2012), https://perma.cc/RL6Q-BEA7.

147 *Cf.* Steven E. Feldman & Sherry L. Rollo, *Extraterritorial Protection of Trade Secret Rights in China: Do Section 337 Actions at the ITU Really Prevent Trade Secret Theft Abroad?*, 11 J. MARSHALL REV. INTELL. PROP. L. 522, 47 (2012); Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 253–54 (2010); Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 475–76 (2012).

148 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS].

149 *Id.* at § 7, art. 39(1).

150 *See* Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154.

151 *Cf.* Aaron Stanley, *US Challenges China Over Compliance with WTO Ruling*, FIN. TIMES (Jan. 13, 2014), https://perma.cc/3H2W-8E3U.

152 *See* Judith Hippler Bello, *The WTO Dispute Settlement Understanding: Less is More*, 90 AM. J. INT'L L. 416, 416–18 (1996).

153 KENNETH J. VANDEVELDE, U.S. INTERNATIONAL INVESTMENT AGREEMENTS 214 (2009).

to enhancing cybersecurity and building a law of cyber peace coupled with relevant analogies from public international law.

III. THE PUBLIC INTERNATIONAL LAW OF CYBER PEACE

Although the private law of cyber peace offers a number of helpful insights regarding ways to enhance global cybersecurity law and policy by harnessing this patchwork of tools, model laws, and data on State practice, it is vital to not ignore the public law of cyber peace. Indeed, this is the body of law with the longest history in regulating global commons spaces, and thus it is important to review it to understand what governance gaps may be filled. This Section undertakes this task by proceeding as follows: First, analogies from arms control regimes are considered, focusing on the interwar years and the nuclear war context. Second, global commons regimes are explored, including space, Antarctica, climate change, and the law of the sea. Third and finally, related regimes including MLATs, extradition treaties, and custom, are explored before moving on to discuss how the public law of cyber peace may be combined with private international law to create the legal foundation for a global culture of cybersecurity.

A. Applying Arms Control Regimes

Arms control treaties have long helped limit the risk of conflict escalation across an array of contexts, to varying degrees of success. This Section investigates the history of two such efforts focusing on the interwar years between World War I and World War II and efforts to reign in the proliferation of nuclear weapons.[154] Although negotiated in different contexts during varied historical epochs, parallels and cautionary tales are drawn to the cybersecurity arena.

1. Interwar Arms Control: Being Cognizant of the Roots of Cyber Conflict.

Following the disastrous results of World War I, with millions of armed forces casualties,[155] the great powers embarked on an effort to limit the size of their own and antagonistic armed forces to limit the risk of future global armed conflict. The resulting major arms control treaties of the 1920s and 1930s primarily determined national strength in terms of fleet size.[156] This changed in

---

154 An earlier version of this research was first published in SHACKELFORD 263–311, *supra* note 10; Shackelford, *From Net War to Nuclear War*, *supra* note 14, at 216–19.

155 *See Viewpoint: 10 Big Myths About World War One Debunked*, BBC (Feb. 25, 2014), https://perma.cc/V99P-RVSP.

156 *See* Caroline F. Ziemke, *Peace Without Strings? Interwar Naval Arms Control Revisited*, 15 WASH. Q., Autumn 1992, at 87 (1992).

the post-World War II period, when "strategic nuclear capability . . . replaced fleets as the measure of global power status."[157] However, the interwar years do convey "an image of a policy environment not unlike our own today," replete with the military grappling with the consequences of a technological revolution built on new products such as fighter planes, submarines, and tanks (as opposed to IT during the modern Revolution of Military Affairs), along with the complexities of navigating multipolar politics.[158]

The interwar arms control regime was based on the 1922 Washington Treaty that placed limits on naval fleet sizes, and was followed by a slew of other treaties designed to ward off another arms race.[159] They failed. Why?[160] Among the lessons learned from this experience by scholars was that "by ignoring underlying sources of conflict, technical agreements may exacerbate insecurity."[161] An example is the 1930 London Naval Treaty, which "reaffirmed Japan's defensive superiority in the Pacific," but failed to address Western and Japanese policy differences toward a unified China.[162] Thus, whereas cyber arms control is not necessarily impossible, to effectively keep the relative cyber peace, agreements must be as comprehensive as possible and take into account the likely reasons that a cyber conflict would start. A cyber weapons treaty would do little good, for example, if negotiators ignored its status during an armed conflict or the geopolitical context in which a conflict could arise, such as U.S.-China relations over Taiwan, or an attributed attack on critical infrastructure. Consequently, the interwar arms control treaties provide a fruitful cautionary tale for what can happen when good intentions race ahead of good policy that takes realpolitik into account for future agreements.

2. The Analogy of Nuclear War.

According to Jim Lewis of the Center for Strategic and International Studies, we understand nearly as much about the relationship between cyber conflict and international security now as we did about strategic thinking related to nuclear weapons in the early 1950s.[163] Assuming that is the case, then it may be helpful to briefly consider the conventions and applicable case law on nuclear warfare to frame contemporary efforts aimed at controlling cyber weapons. During the 1950s

---

157 *Id.*

158 Robin Ranger, *Learning from the Naval Arms Control Experience*, 10 WASH. Q. 47 (1987) (writing in the 1980s, but still with some application to the present).

159 EMILY O. GOLDMAN, SUNKEN TREATIES: NAVAL ARMS CONTROL BETWEEN THE WARS 33–34 (1994).

160 *See* Sean Watts, *Regulation-Tolerant Weapons, Regulation-Resistant Weapons, and The Law of War*, 91 INT'L L. STUD. 540, 540 (2015).

161 Goldman, *supra* note 159, at 30.

162 *Id.*

163 James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, CTR. STRATEGIC & INT'L STUD. 2 (Oct. 2009), https://perma.cc/Y7GD-5MT8.

and 1960s, nuclear policy was a tightly veiled secret with relatively little public discussion,[164] similar to early debates on state-sponsored cyber attacks.[165] That was until Herman Kahn's books, including *On Thermonuclear War* and *Thinking About the Unthinkable*, began a renaissance in scholarly work on the topic that had a great impact on U.S. nuclear policy.[166] The most significant legal decision on the use of nuclear weapons came in 1994, when the U.N. General Assembly voted to submit a request for an advisory opinion to the ICJ on the question of "whether the threat or use of nuclear weapons would be lawful."[167] The U.S. argued in the case that nuclear weapons cannot be banned in the abstract, but rather each case "must be examined individually."[168] Ultimately, the ICJ stated that the threat or use of nuclear weapons "would generally be contrary to the rules of international law."[169] However, the court did not define whether "the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defense, in which the very survival of a State would be at stake."[170] Even though the ICJ did not declare all nuclear weapons illegal, the logic of its holding, that "methods and means of warfare . . . which would result in unnecessary suffering to combatants, are prohibited,"[171] is applicable to cyber conflict given the interconnectivity of cyberspace and resulting potential for damage as seen in attacks like Stuxnet.[172]

The ICJ has not explicitly considered the legality of cyber weapons to this point.[173] Custom, as was mentioned in Section II, requires widespread State practice that is undertaken out of a sense of legal obligation.[174] State practice in the aftermath of cyber attacks seems to suggest a lack of consensus on how best to respond. Consider the initial reaction, or lack thereof, from states including Iran

---

164 *See* NATIONAL ACADEMIES, *supra* note 9, at xi.

165 *See, for example*, Kenneth Corbin, *How Should the U.S. Respond to State-Sponsored Cyberattacks?*, CIO (July 29, 2015), https://perma.cc/7VPR-RPDS.

166 *See generally* HERMAN KAHN, ON THERMONUCLEAR WAR (1960); HERMAN KAHN, THINKING ABOUT THE UNTHINKABLE (1962).

167 FOREIGN & INT'L LAW COMM., N.Y. COUNTY LAWYERS' ASS'N (NYCLA), ON THE UNLAWFULNESS OF THE USE AND THREAT OF NUCLEAR WEAPONS 5 (2000) [hereinafter NYCLA, UNLAWFULNESS OF NUCLEAR WEAPONS], https://perma.cc/HZG2-ESH6.

168 *Id.* at 4.

169 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, at 266 (July 8).

170 *Id.*

171 *Id.* at 262.

172 Lewis, *supra* note 163, at 4.

173 *See* Legality of Nuclear Weapons, *supra* note 169, at 262.

174 *See* North Sea Continental Shelf (Green./Den. v. Neth.), 1969 I.C.J. 41, at 72 (Feb. 20); *Assessment of Customary International Law*, INT'L COMM. OF THE RED CROSS, https://perma.cc/P8V5-VVYD ("To establish a rule of customary international law, State practice has to be virtually uniform, extensive and representative.").

following Stuxnet.[175] However, the fact that States often attempt to hide their cyber activities through intermediaries or otherwise obfuscate could be understood as implicitly acknowledging the unlawfulness of the actions. It may also suggest a growing recognition that certain cyber attacks breach the customary international law norm of nonintervention as seen in recent G20 and G7 cybersecurity pronouncements discussed further in Section IV.[176] Yet, even in the absence of custom, several treaty regimes may provide a basis for the regulation of some cyber attacks under international law that fall below the armed attack threshold, at least until new regimes come online, including in the global commons context discussed next.

B. Analogizing Global Commons Regimes

As difficult as the regulation of chemical, biological, and nuclear weapons may present, it is even more complex to prohibit the use of cyber attacks under international law, due in no small part to technical challenges, verification issues, and the attribution problem, among other concerns.[177] Nevertheless, some nations, such as Russia, potentially fearing Western digital dominance, are pushing for such an arms control-style cyber treaty.[178] Given the political, technical, and legal difficulties of such an approach, this Subsection instead considers lessons gleaned from other treaty systems governing the global commons that have sought to limit the use of weapons to help build out the law of cyber peace, including arms control treaties during the interwar period, nuclear weapons law, space law, and the Antarctic Treaty System (ATS). The Subsection concludes with an analysis of other applicable accords.

1. Introducing the Global Commons.

A "commons" is a general term meaning "a resource shared by a group of people."[179] The notion of the commons can mean either a "resource system" or

---

175 *But see* Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 2007), https://perma.cc/W3J8-PBKL (discussing state responses to the cyber attacks on Estonia).

176 *Cf.* James Blitz, *UK Becomes First State to Admit to Offensive Cyber Attack Capability*, FIN. TIMES (Sept. 29, 2013), https://perma.cc/JQY4-9ZCF.

177 *But see* Neil C. Rowe et al., *Challenges in Monitoring Cyberarms Compliance*, 1 INT'L J. CYBER WARFARE & TERRORISM 1, 1, 12 (2011) (discussing the challenges of and potential paths to cyber arms control, including making use of digital forensics and usage monitoring to verify compliance).

178 *See* Duncan Hollis, *Should There Be an International Treaty on Cyberwarfare?*, OPINIO JURIS (June 13, 2012), https://perma.cc/4ERH-W2P7 (responding to a *US News*-sponsored debate on the desirability of an international cyber weapons treaty).

179 Charlotte Hess & Elinor Ostrom, *Introduction: An Overview of the Knowledge Commons*, *in* UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 3, 3 (Charlotte Hess & Elinor Ostrom eds., 2006).

"a property rights regime," depending on context.[180] As the term is used here, the notion is that certain areas (such as the sky, relevant in the climate change context) belong to all and should be preserved for posterity instead of private persons or the State exclusively managing the resource.[181] Under international law, "commons" are the exception, not the rule, given that territorial sovereignty has in large part defined international relations and international law since the 1648 Treaty of Westphalia, which ushered in the modern nation-state system.[182] The notion of the global commons posits that there are limits to national sovereignty in certain parts of the world, and that these areas should be "open to use by the [international] community but closed to exclusive appropriation" by treaty or custom.[183] At its height, the global commons comprised nearly seventy-five percent of the earth's surface, including the high seas and Antarctica, as well as outer space, the atmosphere, and some argue, cyberspace.[184] Some of these regions were gradually regulated to a greater or lesser extent not by individual countries, but by the international community at times through the vague Common Heritage of Mankind (CHM) concept.[185] More recently, this trend has reversed itself; for instance, individual coastal nations, rather than the international community, now control the vast majority of readily accessible offshore resources.[186] The same trend might be playing out in cyberspace where many nations are seeking to assert greater control online, further challenging the notion of cyberspace as a commons.[187] Indeed, is cyberspace really still a commons, and for that matter, was it ever? Or is it being enclosed to such an extent that it is becoming a form of private property, or even an extension of national territory? Fundamentally, who enjoys sovereignty in cyberspace, and how might it be exercised? And why do these distinctions matter for cybersecurity?[188] These are the questions that drive the analysis of the "cyber pseudo-commons," necessitating an analysis of other global commons regions to glean governance best practices. These examples are framed around historic lessons and policy options from each applicable regime,

---

180 *Id.* at 5.

181 *See, for example*, J. E. S. Fawcett, *How Free Are the Seas?*, 49 INT'L AFF. 14, 14 (1973).

182 *See* Leo Gross, *The Peace of Westphalia, 1648–1948*, 42 AM. J. INT'L L. 20, 20, 26 (1948).

183 CHRISTOPHER C. JOYNER, GOVERNING THE FROZEN COMMONS: THE ANTARCTIC REGIME AND ENVIRONMENTAL PROTECTION 222 (1998); Geert van Calster, *International Law and Sovereignty in the Age of Globalization*, INT'L L. & INST., at 2–3, https://perma.cc/CZ8R-VKW8.

184 *See, for example*, Mark E. Redden & Michael P. Hughes, NAT'L DEF. UNIV., SF NO. 259, GLOBAL COMMONS AND DOMAIN INTERRELATIONSHIPS: TIME FOR A NEW CONCEPTUAL FRAMEWORK?, 1–3 (2010), https://perma.cc/54CY-8DAS .

185 *See* KEMAL BASLAR, THE CONCEPT OF THE COMMON HERITAGE OF MANKIND IN INTERNATIONAL LAW xix–xx (1998).

186 *Id.* at 225–26.

187 *See* Paul Tassi, *The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable*, FORBES (Oct. 2, 2012), https://perma.cc/L672-8BLK.

188 For more on these topics, *see* SHACKELFORD *supra* note 10, at 52–110.

which are in turn summarized in Section IV as part of a polycentric approach to building out a law of cyber peace.

2. From the Digital Frontier to the Final Frontier: Arms Limitation in Space Law as an Analogy for Cyber War.

Outer space is inherently similar to cyberspace; both are vast areas encompassing both territorial and extraterritorial components. Like the weapons systems that have been developed to attack satellites, cyber attacks could have a large-scale strategic impact, both on terrestrial and orbiting assets.[189] In short, the use of either anti-satellite or sophisticated cyber weapons can be game changers. More broadly, both outer space and cyberspace are domains in which intelligence gathering has been widely tolerated, even though the outcry has been greater in the case of cyber espionage than orbital reconnaissance.[190] The nature of cyberspace also makes tracking difficult, because even though the physical Internet is routed in particular jurisdictions, controlling the packets of information that comprise cyberspace is another matter.[191] Similarly, "[s]pacecraft and satellites in orbit pass above many different sovereign jurisdictions,"[192] similar to the myriad jurisdictions through which cyber attacks transit.[193]

Space and telecommunications systems are intertwined with cyberspace, including in such areas as imagery collection, navigation, and signals intelligence, to say nothing of sustainable use discussed further below.[194] However, space law's failure to address whether the legal regime applies during an armed conflict limits its utility as applied to promoting cyber peace. Moreover, the military use of space was not forbidden by the OST, while, according to the Department of Defense (DOD), "[t]here is no legal prohibition against developing and using space control weapons,"[195] for example, save for placing nuclear weapons or other weapons of

---

189 NATIONAL ACADEMIES, *supra* note 9, at 296–97.

190 *See, for example*, James W. Gabberty, *Understanding Motives of Recent Cyber Attacks Against US*, HILL CONG. BLOG (Mar. 11, 2013), https://perma.cc/5LML-TTNL.

191 For more on this topic, *see* SHACKELFORD, *supra* note 10, at 52–110.

192 Julie J. C. H. Ryan, Daniel J. Ryan, & Eneken Tikk, *Cybersecurity Regulation: Using Analogies to Develop Frameworks for Regulation*, *in* INTERNATIONAL CYBER SECURITY LEGAL & POLICY PROCEEDINGS 76, 89 (Eneken Tikk & Anna-Maria Talihärm eds., 2010).

193 *See* THOMAS GRAHAM JR. ET AL., SPY SATELLITES AND OTHER INTELLIGENCE TECHNOLOGIES THAT CHANGED HISTORY 36–38 (2007); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (entered into force Oct. 10, 1967) [hereinafter OST]; NATIONAL ACADEMIES, *supra* note 9, at 296–97.

194 U.S. DEP'T DEF., OFF. GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 26 (2d ed. 1999) [hereinafter DOD ASSESSMENT]; U.S. DEP'T DEF., CYBERSPACE POLICY REPORT 9 (2011).

195 DOD ASSESSMENT, *supra* note 194, at 31.

mass destruction (WMDs) into orbit.[196] A growing list of nations is developing space weapons.[197] Vision for 2020, a 1998 U.S. government report, explains that the U.S. should dominate space, a view shared by retired General Joseph W. Ashy, formerly of U.S. Space Command, who has said: "It's politically sensitive, but it's going to happen . . . we're going to fight *in* space."[198]

International efforts to form a legal regime for space weapons have been nearly as happenstance as those aimed at limiting cyber weapons.[199] Russia and China have advocated for an expanded regime to control both space and cyber weapons.[200] Yet unlike the sophisticated infrastructure and advanced technology needed to develop and deploy space weapons, nearly all nations participate in the Information Age to some degree, whereas only some eighty nations have engaged in space exploration, and fewer still could be considered actively spacefaring.[201] Barring a major conflict, most States do not expect or have the resources "to be either an attacker or a defender" in space in the near term.[202] In contrast, nearly "all states can reasonably expect to be both"[203] an attacker and defender in cyberspace to some degree, which can make reaching consensus difficult.

In summary, analogizing space law illustrates that it is possible to regulate an area of the global commons to bar the most egregious military weapons systems, as this regime has done with nuclear weapons placed in orbit. Space law, however, does not fit the mold of cyber peace given the prevalence of cyber attacks, none of which are equivalent to a WMD attack.[204] There is no cyber equivalent of a nuclear weapon—no single attack now known that can, by itself, bring a country to its knees.[205] A more apt analogy may be the collective action problem of space junk. Some estimates place the total number of objects capable of damaging a

196 OST, *supra* note 193, at art. 4.

197 *See* Jeremy Hsu, *Is a New Space Weapon Race Heating Up?*, SPACE.COM (May 5, 2010), https://perma.cc/8B5E-D9FX.

198 Karl Grossman & Judith Long, *Waging War in Space*, THE NATION (Dec. 9, 1999), https://perma.cc/6U5B-C9EN (emphasis in original).

199 *See, for example,* Turner Brinton, *Obama's Proposed Space Weapon Ban Draws Mixed Response*, SPACE.COM (Feb. 4, 2009), https://perma.cc/42FK-NQY9.

200 *See* Press Release, General Assembly, Prevention of Outer Space Arms Race, Ratification of Nuclear Test-Ban Treaty Among Issues Addressed by Texts Introduced in First Committee, U.N. Press Release GA/DIS/3233 (Oct. 15, 2002), https://perma.cc/J49G-XXPX; Hollis, *supra* at note 178.

201 *See The 10 Countries Most Active in Space*, AEROSPACE-TECHNOLOGY.COM, *available at* https://perma.cc/6Z92-XSVL (last visited on May, 17, 2017).

202 DOD ASSESSMENT, *supra* note 194, at 48.

203 *Id.*

204 Other space law treaties relating to liability claims resulting from space activities, registration of objects launched into space, the governance of the Moon, or satellite regulations have little if any applicability to cyber attacks and so are beyond the bounds of this study.

205 Steven Cherry, *Sons of Stuxnet*, IEEE SPECTRUM (Dec. 14, 2011), https://perma.cc/KW8X-MDY7.

spacecraft at more than thirty-five million, making attribution difficult.[206] As with a stray bolt damaging a satellite, a piece of malware can wreak havoc with disparate websites and networks. As of 2015, however, there has been little multilateral agreement on how to better manage orbital debris, though limited polycentric initiatives have been undertaken that could be informative to cyber peacebuilding.[207] Instead of finding analogies to ban certain types of code then, might it be possible (and desirable) to regulate *all* cyber attacks under public international law?

3. Freeze the Code: The Antarctic Treaty System Approach to Cyber Attacks.

Rather than banning only certain types of cyber attacks, another (admittedly difficult and complex) option to consider is regulating all cyber attacks. The Antarctic Treaty, which besides managing a continent was the first arms control treaty of the Cold War, provides a fruitful analogue because it goes further than the OST and bans *all* military activities.[208] The main objective of the Antarctic Treaty System (ATS) is to ensure "that Antarctica shall continue forever to be used exclusively for peaceful purposes."[209] Like Antarctica, the Internet is a rich resource, being a repository of knowledge and a vital channel for commerce and communications. However, imposing a freeze on developing new software that could be used to launch malicious exploits, even if it were possible, would likely not be preferable given that it could stifle innovation, among other legitimate concerns.[210] Nor would a traditional international accord likely be capable of keeping up with rapidly changing IT, necessitating a kind of standing public-private committee of cybersecurity experts that could analyze industry best practices and help identify new security threats as they arise. Subsequent enforcement and coordination would thereafter pose daunting challenges. On the surface, then, it appears that neither barring certain malignant code nor all possible variations of cyber attacks under international law is an effective, efficient

---

206 *See* Ronald L. Spencer, Jr., *International Space Law: A Basis for National Regulation*, *in* NATIONAL REGULATION OF SPACE ACTIVITIES 1, 4 (Ram S. Jakhu ed., 2010).

207 *See* Frank A. Rose, Remarks at the UN Institute for Disarmament Research, Space Security Conference, in Geneva, Switzerland: Laying the Groundwork for a Stable and Sustainable Space Environment (Mar. 29, 2012), https://perma.cc/6CLN-MY7T; COPUOS Space Debris Mitigation Guidelines (2010), U.N. OOSA, https://perma.cc/4T99-E866 (last visited Nov. 11, 2013); Scott J. Shackelford, *Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris*, 51 AM. BUS. L.J. 429, 430 (2014).

208 Antarctic Treaty art. 1, ¶ 1, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 72 (defining "peaceful purposes" in Antarctica as banning "any measures of a military nature").

209 *Id.* at pmbl.

210 *See, for example*, Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INST., at 12, https://perma.cc/P9HY-UQKD.

response to the cyber threat without substantial technological improvements.[211] What then about the potential of using either atmospheric governance or international communications to prosecute attackers and their facilitators?

4. On Climate Change and Cyber Attacks.

It is difficult to think of two issues with a greater potential to negatively impact both our natural environment and the global economy than climate change and cyber attacks. Though the long-term estimates on both are notoriously hard to pin down, contested estimates on the cost of cyber attacks range from approximately $400 billion for 2014 to more than $3 trillion by 2020.[212] Similarly, the cost of climate change has been estimated at some $1.2 trillion annually, which works out to roughly 1.6 percent of global GDP.[213] Moreover, although the atmosphere and cyberspace are distinct extraterritorial arenas, they share similar problems of overuse, difficulties of enforcement, and the associated challenges of collective inaction and free riders.[214] It is also true that actions taken by a multiplicity of actors on different governance scales (from local to global) can impact both the global climate change problem and the cause of promoting cyber peace. This is part and parcel of the literature on polycentric governance—sometimes called the Bloomington School of Political Economy—which is quickly coming into vogue as the preferred model of tackling "new" global collective action problems, marking a shift from twentieth century models of global commons governance and is discussed further in Section IV.

Applying the complete corpus of international environmental law, or even that segment focusing on atmospheric governance, is beyond the scope of this Article.[215] However, there are targeted lessons from the ongoing climate change negotiations that deserve attention, beginning with the Montreal Protocol before moving on to the Twenty-First U.N. Framework Convention on Climate Change (UNFCCC) Conference of the Parties (COP21) 2015 meeting in Paris.[216]

Much like Rachel Carson's *Silent Spring* helped jumpstart a global conversation about the state of environmental protection, and Garrett Hardin's article *The Tragedy of the Commons* helped popularize the dangers of open access regimes, another article, this time by three British scientists, helped precipitate

---

211 *But see* Rowe et al., *supra* note 177, at 12 (making the case that cyber arms control is possible using current technology).

212 *See, for example*, *Net Losses: Estimating the Global Cost of Cybercrime*, CSIS at 2 (2014), https://perma.cc/75GL-V54K; *Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020*, TECH. REP. (Feb. 20, 2014), https://perma.cc/RTC2-VF9W.

213 *See* Fiona Harvey, *Climate Change is Already Damaging Global Economy, Report Finds*, GUARDIAN (Sept. 15, 2012), https://perma.cc/2WEP-89TW.

214 *See* Ostrom, *supra* note 31.

215 For more on this area, see Shackelford & Fort, *Sustainable Cybersecurity*, *supra* note 16.

216 *See* Paris Agreement, EUR. COMM'N, https://perma.cc/QC2E-L6J6.

arguably the most successful international treaty in history—the Montreal Protocol—which, in 2009, became the first U.N. treaty to achieve universal ratification after the U.N. Charter itself.[217] Why has the Montreal Protocol been so successful, and what lessons does it hold for climate change and for that matter cybersecurity? In short, the science was clear, scarcity was plain, alternatives were available, and geopolitics was simpler.[218] This state of affairs stands in opposition to how the climate change context during the UNFCCC COP process, which were long mired in geopolitical, international economic, and security challenges, as were brought into sharp relief at COP15 in 2009.[219] COP21 succeeded where COP15 failed largely because of the high number of serious national climate pledges on the lead up to the conference itself, with the U.S.-China announcement on bilateral emissions reductions leading the way.[220] By July 2015, nearly five months before COP21 would convene, more than a dozen nations, plus the E.U., had made climate pledges, with many more to come.[221] Analogizing atmospheric governance to promoting cyber peace, a push could be made to follow the COP21 approach in the cyber context and encourage transparency, such as by nations announcing pledges that best fit their unique national circumstances ahead of multi-stakeholder cybersecurity forums. The U.S.-China G2 Cybersecurity Code of Conduct is a helpful step forward in this direction, as are the G20 and G7 cybersecurity pronouncements discussed further in Section IV.

5. Applying the Law of the Sea to Promote Cyber Peace.

The Law of the Sea (LOS), like outer space, Antarctica, and the atmosphere, enjoys parallels with cyberspace. The codification process that resulted in the first United Nations Convention on the Law of the Sea (UNCLOS) treaty began in 1945, leading to UNCLOS I in 1958.[222] However, UNCLOS I did not sufficiently address concerns about the legal status of the deep seabed lying underneath the high seas, highlighting the need for further negotiations.[223] Relatively little was accomplished at UNCLOS II due to geopolitical divides.[224] This served as an

---

217 *See* Key Achievements of the Montreal Protocol to Date, ZONE SECRETARIAT, https://perma.cc/7BVF-2QJR.

218 For more on this topic, see Shackelford, *On Climate Change and Cyber Attacks*, *supra* note 16.

219 *See Key Powers Reach Compromise at Climate Summit*, BBC NEWS (Dec. 19, 2009), https://perma.cc/BX4K-U3KP.

220 WHITE HOUSE, FACT SHEET: U.S.-CHINA JOINT ANNOUNCEMENT ON CLIMATE CHANGE AND CLEAN ENERGY COOPERATION, https://perma.cc/M6TU-26LL.

221 *See* Nell Greenfieldboyce, *U.N. Holds Climate Talks In New York Ahead Of Paris Meeting*, NPR (June 29, 2015), http://www.npr.org/2015/06/29/418641168/u-n-holds-climate-talks-in-new-york-ahead-of-paris-meeting.

222 SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 85 (1998).

223 *See* Christopher C. Joyner, *Antarctica and the Law of the Sea: An Introductory Overview*, 13 OCEAN DEV. & INT'L L. 277, 281 (1983); BUCK, *supra* note 222, at 86.

224 BUCK, *supra* note 222, at 86.

impetus for UNCLOS III, which was tasked with regulating the use, exploration, and exploitation of all living and non-living resources of the high seas,[225] a vast area comprising more than seventy percent of the planet's surface.[226] Still, the role of the private sector remained truncated, a cautionary tale when considering paths toward revamping Internet governance to promote cyber peace. As the deep seabed mining provisions of UNCLOS proved unsatisfactory to the developed world, the treaty was amended in 1994 to better comport with private economic development,[227]provisions that are now being put to the test with the uptick in deep seabed exploration by mining firms.[228]

Among the provisions of UNCLOS III that may be applied to cybersecurity include Article 19, which states that a nation should not use another "nation's territorial sea to engage in activities prejudicial to the peace, good order, or security of the coastal State."[229] This prohibition includes the collection of information, distribution of propaganda, or interference with systems of communications[230]—provisions that have direct application to such exploits as Distributed Denial of Service (DDoS) attacks. Moreover, Article 113 requires domestic criminal legislation to punish willful damage to submarine cables,[231] which represent the fiber-optic circulatory system of the global Internet. Depending on how broadly "damage" is conceived,[232] an argument could be made that the Article 19 prohibition should also apply to Article 21 and 113 claims involving submarine cables.[233] This could mean that, depending on State practice, cyber attackers who send code through submarine cables that come to shore in coastal States could be in breach of UNCLOS. However, this does not include enforcement mechanisms beyond calls for domestic criminal legislation, highlighting the need for State practice to mirror international treaty obligations if the law of cyber peace is to be an effective deterrent to cyber attackers.

---

225 *Id.* at 50, 87.

226 *How Much Water is There On, In, and Above the Earth?,* U.S. GEOLOGICAL SERV., https://perma.cc/W6AG-YVAY.

227 BUCK, *supra* note 222, at 91; Agreement Relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea of 10 December 1982, § 5, July 28, 1994, S. Treaty Doc. No. 103-39, 1836 U.N.T.S. 41; *see* David Shukman, *Deep Sea Mining 'Gold Rush' Moves Closer*, BBC (May 17, 2013), https://perma.cc/K2JC-EC5Q.

228 *See U.N. Body Issues Exploration Contracts as Era of Deep Seabed Mining Nears*, JAPAN TIMES (July 25, 2015), https://perma.cc/7USX-GJHQ.

229 United Nations Convention on the Law of the Sea, art. 19, ¶1, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]; DOD ASSESSMENT, *supra* note 194, at 34.

230 UNCLOS, art. 19(1)(c)–(d), (k).

231 *Id.* art. 113. *See also* art. 21(1)(c) (granting coastal states the option of passing laws to protect cables and pipelines); DOD ASSESSMENT, *supra* note 194, at 37 (expanding on these arguments).

232 UNCLOS, at art. 19(1).

233 *See* DOD ASSESSMENT, *supra* note 194, at 37.

UNCLOS is also an important example of a regime that was unsuccessful until it better recognized the needs of the private sector. Both proposed and existing legal regimes being applied to strengthen cyber peace should similarly ensure sufficient protections for private enterprise to promote engagement and spur innovation by not sidelining private entities as Internet governance evolves.[234] Relatedly, the history of UNCLOS also underscores the importance of including non-state actors and effective public-private partnerships in polycentric efforts aimed at managing global common pool resources,[235] including the Internet.

C. Considering Other Applicable Accords

Building from the analysis of global commons regimes, this final Subsection investigates the utility of other applicable public accords—focusing on international telecommunications law, MLATs, and extradition treaties—before moving on to an analysis of governance gaps undertaken in Section IV.

1. International Communications Law and Cyber Attacks.

In many ways, the development of international communications law was the direct precursor to cyber law, beginning with agreements dating from the 1800s designed to protect the first submarine cables.[236] A key focal point for modern telecommunications governance is the ITU, the oldest still-active intergovernmental organization in the world.[237] For more than 150 years, the ITU has been the primary organization responsible for multilateral telecom governance,[238] and more recently it has also played a role in Internet governance.[239] The ITU Convention militates against "harmful interference," defined in Annex 3 of the document as that which "endangers . . . *safety services*, or seriously degrades, obstructs or repeatedly interrupts a radio communication service."[240] "Safety services" include technologies "used permanently or temporarily for the safeguarding of human life and property," which could conceivably refer to public services such as health, police, and public transport, along with critical

---

234 JOHN D. NEGROPONTE ET AL., DEFENDING AN OPEN, GLOBAL, SECURE, AND RESILIENT INTERNET 14 (Council on Foreign Rel. Independent Task Force Rep. No. 70, 2013).

235 *See* BUCK, *supra* note 222, at 91.

236 *See* DOD ASSESSMENT, *supra* note 194, at 4, 32–33.

237 *See International Telecommunication Union*, U.N., https://perma.cc/J7AR-EYS2.

238 *See* CHARLES H. KENNEDY & M. VERONICA PASTOR, AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATIONS LAW 30–33 (1996).

239 For more on this topic, see SHACKELFORD, *supra* note 10, at 3–51, 312–66.

240 International Telecommunications Convention, Nairobi, annex 2, Nov. 6, 1982, 32 U.S.T. 3821 (emphasis added).

infrastructure more generally, all of which are vulnerable to cyber attacks.[241] However, the lack of mandatory enforcement mechanisms and its failure to apply during armed conflicts limits the efficacy of this regime, as does political resistance from some stakeholders to empower the ITU to have a larger role in enhancing global cybersecurity.[242]

The ITU Convention also gives governments wide discretion in regulating private activity that "may appear dangerous to the security of the State,"[243] including acts "contrary to . . . public order, or to decency."[244] Such broad authority opens the door to a wide range of domestic regulatory interventions in Internet governance. Indeed, at least according to the U.S. DOD, international communications law currently "contains no direct and specific prohibition" against the use of cyber attacks "by military forces, even in peacetime."[245] As a result, whereas elements within the ITU Charter may help the international community manage cyber attacks, it offers limited guidance in promoting cyber peace without additional support.

2. Mutual Legal Assistance Treaties.

Numerous bilateral and multilateral treaties dealing with everything from legal assistance, extradition, diplomatic relations, and friendship, to status of forces agreements, also include provisions that impact cybersecurity. The U.S., for example, is party to dozens of MLATs that could be used to seek criminal prosecution of cyber attackers, especially those MLATs that either explicitly mention IT or are termed broadly enough to cover *all* law enforcement investigations.[246] However, there are often no enforceable obligations under these treaties, limiting their utility, as seen in the 2007 alleged Russian cyber attacks on Estonia, and the 2013 episode regarding Russian President Vladimir Putin's refusal to extradite accused NSA leaker Edward Snowden to U.S. authorities despite the presence of a U.S.-Russia MLAT.[247] The U.S. is also "a party to more than a hundred bilateral extradition treaties."[248] Without such accords, national

---

241 *Id.* at n.1.

242 *But see* GLOBAL CYBERSECURITY INDEX, *supra* note 109 (representing an effort by the ITU to enhance the transparency of global cybersecurity governance).

243 DOD ASSESSMENT, *supra* note 194, at 33–34.

244 Constitution of the International Telecommunications Union, art. 34, Dec. 22, 1992, https://perma.cc/SS4V-EHTV.

245 *Id.* at 34.

246 *See, for example*, U.S.–CANADA MLAT, S. TREATY DOC. NO. 100–14; 100th Cong., 2nd Sess. Exec. Rept. 100–28; 100th Cong, 2nd Sess. Exec. Rept 101–10; 101st Cong., 1st Sess. XXIV ILM No. 4, 7/85, 1092–99.

247 *See* U.S.–Russia MLAT, S. TREATY DOC. NO. 106–22 (1999).

248 DOD ASSESSMENT, *supra* note 194, at 33; *see* U.S. TREATIES OF EXTRADITION, CORNELL UNIV. LAW SCHOOL, at 6–9, https://perma.cc/T8XQ-FA5L.

governments would "have neither an international obligation nor the domestic authority to deliver custody of an individual" for prosecution in a foreign jurisdiction.[249] These treaties could be amended to more effectively bring the perpetrators of cyber attacks to justice, such as by including incentives for information sharing, sanctions for noncompliance, and making their coverage more explicit. There is, in fact, an effort to update the U.S.-U.K. MLAT along these lines.[250] States may be willing to expend the political capital to make these revisions due to the gravity of the cyber risk that they face, along with the increasing clarity surrounding the extent of interconnection within the global networked commons.

3. Extradition Treaties and Diplomatic Relations.

Another avenue to promote cyber peace would be to leverage existing treaties to help safeguard certain tempting targets such as embassies. The 1961 Vienna Convention on Diplomatic Relations enshrines the right of "inviolability of the premises" of a diplomatic mission, its archives, private residences and property of its agents, and its communications.[251] Applied to the law of cyber peace, then, this regime could protect all transmissions made to and from government embassies and missions against cyber attacks or espionage. This regime would be applicable in attacks that have already been waged against Russian and Japanese embassies, among others.[252] The reverse has also occurred, such as when the U.S. declared Venezuela's consul general a persona non grata after she allegedly planned cyber attacks against U.S. networks.[253] Still, some countries are not relying on such legal instruments to protect themselves, such as Estonia, which has taken the proactive step of creating a "virtual embassy" to back up its citizens' data outside of its geographic borders.[254]

Treaties of friendship, commerce, and navigation could also be used to leverage the prospects for cyber peace.[255] Other applicable frameworks to a law

---

249 DOD ASSESSMENT, *supra* note 194, at 35.

250 *See, for example*, Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. INTERNET & SOC'Y (Feb. 23, 2015), https://perma.cc/3E45-Q8Y7.

251 *Id.* at 38; *see* Vienna Convention on Diplomatic Relations, arts. 2, 24, 27, 30, Apr. 18, 1961, 23 U.S.T. 3227, https://perma.cc/99QD-F6VX.

252 *See, for example*, Eduard Kovacs, *DDoS Attack Targets Russian Embassy Website*, SOFTPEDIA (Sept. 12, 2011), https://perma.cc/2APU-AXWK; *Cyber War on Japanese Embassies*, EXPATICA (Oct. 26, 2011), https://perma.cc/ST43-5DPZ.

253 *See US Expels Venezuela's Miami Consul Livia Acosta Noguera*, BBC (Jan. 9, 2012), http://perma.cc/NWC8-NF2R.

254 *See* IMPLEMENTATION OF THE VIRTUAL DATA EMBASSY SOLUTION, ESTONIAN MINISTRY OF ECONOMIC AFF. & COMM., http://perma.cc/73P8-QJ3R.

255 *See* DOD ASSESSMENT, *supra* note 194, at 39.

of cyber peace include countermeasures allowing states to respond to violations,[256] several U.N. General Assembly resolutions relating to cybersecurity,[257] and limited regional initiatives such as NATO's cybersecurity efforts, along with the Council of Europe, Organization of American States, and Shanghai Cooperation Organization's cybersecurity initiatives.

IV. TOWARD A COMBINED LAW OF CYBER PEACE: A POLYCENTRIC PATH FORWARD

Section III undertook a wide-ranging, non-comprehensive investigation into some of the sources of public international law that, together, could be leveraged to help build out the law of cyber peace if the limitations described are overcome. While a patchwork, these regimes together provide a helpful polycentric foundation that could be synergistically refined through additional protocols and public-private partnerships across a range of industries, sectors, and country groupings. To ascertain the promise of such an approach in further building out the law of cyber peace (assuming that new treaty formation remains off the table for geopolitical reasons), Section IV begins by further unpacking the benefits and drawbacks of polycentric governance in the cybersecurity context before moving on to discuss implications for policymakers and managers.

A. The Frontiers (and Limits) of Polycentrism

Increasingly, leaders such as the former President of Estonia, Toomas Ilves; the former Director of the Internet Corporation for Assigned Names and Numbers (ICANN), Fadi Chehadé; and even Nobel Laureates such as Professor Elinor Ostrom have proffered polycentric governance as the best path forward to addressing the global collective action problems of climate change and cyber attacks.[258] Indeed, already some of the public- and private-sector efforts highlighted in this Article may be bearing fruit with, by some estimates, the severity of cyber attacks beginning to plateau and "an emerging norm against the

---

256 *See generally* Schmitt, *supra* note 12 (exploring the contours of available countermeasures under international cybersecurity law).

257 G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010).

258 *See* Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), https://perma.cc/YAU4-8C48.

use of severe state-based cyber tactics" emerging.[259] But it is equally important to consider the evolution and limits of this approach.

It may be easiest to understand polycentric governance in juxtaposition to the alternative—monocentrism, which is a political system where the authority to enforce rules is "vested in a single decision structure that has an ultimate monopoly over the legitimate exercise of coercive capabilities."[260] At its core—building from important notions of legitimacy, power, and multiple decision centers—polycentric governance is concerned with the rule of law. In this manner, the U.S. constitution has been described as an "experiment in polycentricity," with federalism being one way to operationalize the concept.[261] Professor Michael Polanyi did a great deal to develop and advance the field of polycentric governance. In many ways, his approach was original in that it began with a realization as to the importance of social organization in the process of scientific discovery above and beyond strict adherence to the "scientific method."[262] He realized, for example, that polycentric structures are vital for scientific discovery given that the inherent "freedom is utilized to search for an abstract end goal (objective truth)."[263] This can only occur in the absence of an overarching authority in arenas driven by ideals including beauty, truth, and justice in the contexts of art, religion, and the law.[264] In this way, capitalism itself may be seen as polycentric given that it incorporates "a web of many agents that constantly adjust their behavior to the decisions made by others."[265] This may be compared against a monocentric-socialist system in which a centralized command and control authority is tasked with organizing a top-down structure for making production decisions.[266] In such a polycentric system, ideas of equity and justice, Polanyi argued, may only be crystallized by a gradual process of trial-and-error experimentation.[267] Arguably, we are undertaking such experimentation now at the global level, with divergent State and private-sector practice geared toward promoting cyber peace as was discussed in Sections II and III.

Professor Lon Fuller agreed with Polanyi's assessment with regards to polycentrism, arguing that many legal decisions are in fact polycentric in that they involve multiple "decision centers and the network of cause and effect

---

259 Brandon Valeriano & Ryan C. Maness, *The Coming Cyberpeace: The Normative Argument Against Cyberwarfare*, FOREIGN AFF. (May 13, 2015), https://perma.cc/ZF6E-VEGY.

260 Paul D Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237, 244 (2012).

261 *Id.* at 245.

262 *Id.* at 238.

263 *Id.*

264 *Id.*

265 *Id.*

266 Aligica & Tarko, *supra* note 260, at 238.

267 *Id.* at 239.

relationships is not understood very well."[268] Such a conceptualization of the justice system highlights, among other issues, the prevalence of unintended consequences that can frustrate justice seekers.[269] As such, Professor Fuller argued that as the degree of polycentricity in a system increases, judges should be more inclined to leave a decision to either the competitive market or to the political branches.[270] Similar arguments could be made with regards to cybersecurity, especially given the difficulty involved with identifying cybersecurity best practices in a dynamic technological environment. However, debates swirling around a cybersecurity market failure[271] and the relative lack of action by the U.S. Congress on cybersecurity militate against the courts deferring to the other branches.

The Ostroms' work on polycentric governance, begun in the 1960s, was initially centered on questions of metropolitan governance, but subsequently evolved in two directions—social theory, and empirical investigations of governance structures. The Ostroms argued that coordination in complex systems is in fact possible through interorganizational arrangements that "would manifest market-like characteristics and display both efficiency-inducing and error-correcting behavior."[272] In other words, by taking a political economy approach, the Ostroms were able to show that "competition among public agencies is not necessarily inefficient."[273] Yet the great leap in governance research was the Ostroms' contention to test their presumption, "to undertake critical tests where divergent theories imply contradictory conclusions."[274] This was the birth of empirical polycentric governance research, the ramifications of which continue to resonate around the world in a wide array of contexts, including with regards to cybersecurity.

As applied to cybersecurity, the field of polycentric governance has an array of particularized lessons drawn from Professor Ostrom's work, as summarized in her Institutional Analysis and Design (IAD) Framework.[275] This is a framework of governance best practice gleaned from decades of commons field studies and

---

268 *Id.* at 240.

269 *Id.*

270 *Id.*

271 *See* Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12–05, 2012), https://perma.cc/C49M-LGTY (arguing that market failures are not so common in the cybersecurity realm); Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 82 (2011) (making the case against there being a cybersecurity market failure).

272 Aligica & Tarko, *supra* note 260, at 242.

273 *Id.*

274 *Id.*

275 *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 117 (Eric Brousseau et al. eds., 2012).

applied, among other contexts, to global commons issues including atmospheric governance. Some of these principles similarly have resonance to the cause of cybersecurity due diligence, including the need to undertake effective cost-benefit analysis,[276] conduct supply chain monitoring with an eye toward spotting hardware and software vulnerabilities, and institute governance strategies that permit ample space for innovation while still mandating proven best practices.[277] The latter goal may be furthered by, for example, requiring NIST Cybersecurity Framework compliance for all suppliers and potential partners, something that more firms are undertaking. For example, in early 2015, Bank of America announced "that it is using the Framework and will also require it of its vendors," while "QVC is announcing that it is using the Cybersecurity Framework in its risk management."[278]

At a more global level, this approach highlights support for minilateral norm building, which we are already seeing across a number of fora including the G2, G7, and G20. For example, the G2 Cybersecurity Code of Conduct that was mentioned in the introduction calls for mutual restraint in cyber economic espionage, particularly the theft of trade secrets.[279] Similarly, the G7 continued its work on cybersecurity in 2016, publishing its view that "no country should conduct or knowingly support ICT-enabled (information and communication technology) theft of intellectual property" and that all G7 nations should work to "preserve the global nature of the Internet," including the free flow of information in a nod to the notion of cyberspace as a "global networked commons."[280] The 2015 G20 has perhaps been the most active forum pushing, in particular, the international law of cyber peace, stating in a 2015 communique, for example, that: (1) "international law, including the United Nations (UN) Charter, applies to nation-state conduct in cyberspace;" and (2) "no country should conduct or support the cyber-enabled theft of intellectual property."[281] Similarly, the U.S. proposed three peacetime norms that were accepted for inclusion in the 2015 U.N. Group of Governmental Experts consensus report, which includes language

---

276 Cost-benefit analysis in the cybersecurity context is challenging both because of the difficulty in defining all the associated costs of a successful data breach as well as determining an investment strategy to identify and instill technological, budgetary, and organizational best practices. *See, for example*, GREGORY J. TOUHILL & JOSEPH TOUHILL, CYBERSECURITY FOR EXECUTIVES: A PRACTICAL GUIDE 31 (2014).

277 *See* Ostrom, *supra* note 275, at 118 & tbl. 5.3.

278 FACT SHEET: WHITE HOUSE SUMMIT ON CYBERSECURITY AND CONSUMER PROTECTION, https://perma.cc/S68Y-WPJ6.

279 *See* Robinson, *supra* note 7.

280 *G7 Leaders*, *supra* note 6.

281 G20 COMMUNIQUÉ, *supra* note 5.

on protecting critical infrastructure, safeguarding Computer Security Incident Response Teams, and collaborating on cybercrime investigations.[282]

These forums are proving invaluable for minilateral norm building that is helping to crystallize State practice. Overall, this form of polycentric undertaking is similar to efforts like the Guiding Principles on Business and Human Rights (Guiding Principles) Framework approach authored by Professor John Ruggie, which encourages greater stakeholder buy-in from diverse organizations rather than a multilateral, top-down approach to promoting human rights in business practices.[283] Such an approach could also aid in norm building by norm entrepeneurs, such as leading businesses and governments announcing efforts that could eventually cause a "norm cascade" in which cybersecurity best practices become internalized and eventually codified in national and international laws.[284] Ultimately, though, the trick is finding the appropriate "balance between simplicity and complexity" to better leverage the power of polycentric governance to promote cyber peace.[285]

B. Summary and Implications

Taken together, the diverse sources of private and public international law discussed in this Article provide the beginnings of a legal framework to manage cyber attacks during peacetime. The private and public sectors are pioneering systems of cybersecurity due diligence and cyber risk insurance that are already helping to mitigate the cyber risk of an array of small, medium, and large organizations. Existing bilateral and multilateral trade and investment treaties provide the ability for private entities to protect their intellectual property such as through international arbitration. If a host nation's domestic laws criminalize cyber attacks, then applicable MLATs and extradition treaties would apply to make perpetrators accountable in various jurisdictions. If the attack were directed against a foreign mission or embassy, then the Vienna Convention on Diplomatic Immunity would provide certain remedies and potentially reparations to the victim nation, potentially combined with virtual embassy schemes such as the one currently pioneered by Estonia. Moreover, provisions under UNCLOS III

---

282 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly, A/70/174 (July 22, 2015).

283 *See, for example*, JOHN G. RUGGIE, JUST BUSINESS: MULTINATIONAL CORPORATIONS AND HUMAN RIGHTS 78 (2013).

284 *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

285 Michael D. McGinnis, *Elinor Ostrom: Politics as Problem-Solving in Polycentric Settings*, *in* ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY 281, 285 (Daniel H. Cole & Michael D. McGinnis eds., 2014).

regulating submarine cables, the ability to prosecute private parties in breach of the ITU treaty in telecommunications law, and interference with satellite transmissions in space law, all place restrictions on cyber attackers. This regime has been criticized as "patchwork,"[286] partly because of prevalent enforcement and verification concerns.[287] But it is a foundation, however limited, from which to build the edifice of cyber peace.

If political impasses are overcome and State practice further crystallizes, negotiators could craft a new cybersecurity treaty to improve upon the suboptimal status quo that: (1) defines appropriate graduated sanctions against nations harboring or sponsoring cybercriminals and terrorists where possible; (2) clarifies which international legal provisions apply below the armed attack threshold; (3) establishes a regime for attribution that includes robust information sharing; (4) provides for enforcement mechanisms; and (5) provides a system of efficient dispute resolution.[288] Several proposals have been made along these lines, and indeed it may be possible to build on recent norm development, such as from the G20, by requiring a duty to assist victim nations, not interfering with cybersecurity investigations (including first responders), and codifying a prohibition on attacking critical infrastructure.[289]

Ultimately, the limitations of existing regimes, created by analogy and the extension of principles developed to suit different challenges, demonstrate the limits of international laws to enhance cybersecurity. Internet freedom arguments about the "unregulatability of BITs" and the ability of attackers to circumvent national borders remain powerful especially given rapid technological advancements, but have been partly undermined by the work of scholars, such as Professor Joel Reidenberg, who have advocated for the potential of private regulatory regimes to serve as proxies for laws.[290] However, the fundamental difficulty of enforcing regulations in cyberspace remains apparent given problems of attribution, environmental plasticity, and the inter-networked nature of cyberspace, among other challenges.[291] This means that although regulation is possible in cyberspace, it is fraught with difficulties. It is best, then, to consider law and norms alongside market-based incentives and code as part of a polycentric system for fostering cyber peace given the absence of a comprehensive legal

---

286 Finnemore & Sikkink, *supra* note 284, at 859.

287 For more on regime effectiveness in the cybersecurity context, see SHACKELFORD, *supra* note 10; Shackelford, *On Climate Change and Cyber Attacks*, *supra* note 16.

288 *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 880 (2012).

289 Group of Governmental Experts, *supra* note 282.

290 ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 203–04 (2006).

291 *Id.* at 205.

regime. By stacking such regimes, as it were, gaps within one arena may be offset by coverage in another such that more robust coverage results.

What other options exist in enhancing cybersecurity beyond adapting existing treaties? Some argue for the widespread use of preventative self-defense with its attendant dangers of international instability and escalation.[292] Others would prefer a regime of universal jurisdiction, whereby any State would be able to prosecute cyber attackers.[293] An extreme option is a movement toward a surveillance society such that every State would have greater information awareness, raising obvious privacy implications while not necessarily contributing to overall cybersecurity.[294] Among other issues, each of these approaches raises the thorny problem of harmonization, as well as reciprocity. Given that the U.S. remains a leading cyber power, U.S. cybersecurity policy may well be mirrored back; we have to be comfortable with the reflection.

V. CONCLUSION

International law changes with events: as Justice Oliver Wendell Holmes wrote, "The life of the law has not been logic; it has been experience."[295] It is essential for policymakers to consider cyber attacks as the revolutionary threat that they are to the security and welfare of citizens around the world in order for real and lasting progress to be made. But it is equally necessary for scholars, jurists, and negotiators to place a greater emphasis on developing and clarifying the law of cyber peace, given that this legal regime will be responsible for managing responses to the vast majority of cyber attacks.[296] Important work, including *Tallinn 2.0*, has contributed greatly to this effort, but much more remains to be done, particularly with regards to ascertaining the status of customary international cybersecurity law based on data about State practice, and the overall regime effectiveness of various cyber laws. This Article has explored how some existing private and public sources of international law may be applied to promote cyber peace. As has been shown, there is not an absence of law in cyberspace. It is far from the untamed digital Wild West that it is at times made out to be. The issue is one of reconceptualizing cyber attacks and determining appropriate responses within an evolving polycentric system. Existing regimes should not be abandoned, or their value underappreciated, in favor of new cybersecurity accords, given that little clarity exists as to what such treaties might look like, even

---

292 *See* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 858–59 (2001).

293 *See* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 57 (2010).

294 *See* Denver Nicks, *Report: Usefulness of NSA Mass Surveillance 'Overblown*,' TIME (Jan. 13, 2014), https://perma.cc/CP73-FWNW.

295 OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1923).

296 *See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 J. CONFLICT & SEC. L. 187, 187 (2012).

if it was politically feasible to negotiate and ratify them. Better, one might think, to bolster the process of legal clarification and norm building now, and not let the great be the enemy of the good.